МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ УПРАВЛІННЯ
КАФЕДРА МЕНЕДЖМЕНТУ ТА ФІНАНСІВ

До захисту допустити
Зав. кафедри
к.е.н., доцент

_____ **М.О. Горбашевська**

«05» грудня 2024 р.

ЗНИЖЕННЯ РИЗИКІВ ПРИ ВПРОВАДЖЕННІ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кваліфікаційна робота
здобувача вищої освіти другого (магістерського) рівня вищої освіти освітньо-професійної програми «Менеджмент. Управління фінансово-економічної безпеки»
Галишинець Ю.І.
Науковий керівник:
Горбашевська Марина Олексіївна, к.е.н., доцент кафедри менеджменту та фінансів
Рецензент:
Осипенко Кристина Валеріївна, к.е.н., доцент, спеціаліст 2 Управління Головного управління СБУ в Донецькій та Луганській областях

Кваліфікаційна робота захищена
з оцінкою ___відмінно (90/А)___
Секретар ЕК_____
«19» грудня 2024 р.

Київ – 2024

МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ УПРАВЛІННЯ
КАФЕДРА МЕНЕДЖМЕНТУ ТА ФІНАНСІВ

Рівень вищої освіти Магістр
Шифр та назва спеціальності 073 «Менеджмент»
Освітньо-професійна програма Менеджмент. Управління фінансово-економічної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри к.е.н., доцент,
(науковий ступінь, вчене звання)
Горбашевська М.О.
(ПІП завідувача кафедри)
«29» лютого 2024 р.

ПЛАН ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Галишинець Юрій Ігорович
(прізвище, ім'я, по батькові)

1. Тема роботи Зниження ризиків при впровадженні корпоративної інформаційної безпеки керівник роботи Горбашевська М.О., к.е.н., доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом Маріупольського державного університету від «29» лютого 2024 року № 36

2. Строк подання студентом роботи «05» грудня 2024 року

3. Вихідні дані до роботи (мета, об'єкт, предмет)

Мета роботи: дослідження та обґрунтування теоретичних і методичних підходів до впровадження корпоративної інформаційної безпеки, а також розробка практичних рекомендацій для мінімізації ризиків, що супроводжують цей процес.

Предметом дослідження є процеси управління ризиками в контексті впровадження корпоративної інформаційної безпеки.

Об'єктом дослідження є корпоративна інформаційна безпека досліджуємого підприємства.

4. Зміст роботи (перелік питань, які потрібно розробити)

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ ТА ВПРОВАДЖЕННЯ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

1.1. Поняття та класифікація корпоративних інформаційних систем

1.2. Корпоративна інформаційна безпека: її характеристика та складові

1.3. Характеристика ризиків інформаційної безпеки в корпоративній інформаційній системі

РОЗДІЛ 2. ОЦІНКА РИЗИКІВ ПРИ ВПРОВАДЖЕННІ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Організаційна характеристика підприємства ПрАТ «Тернопільський молокозавод»

2.2. Аналіз фінансової та виробничої сфер підприємства в умовах корпоративної інформаційної безпеки

2.3. Оцінка ризиків при впровадженні корпоративної інформаційної безпеки на ПрАТ «Тернопільський молокозавод»

РОЗДІЛ 3 ШЛЯХИ ЗНИЖЕННЯ РИЗИКІВ ПРИ ВПРОВАДЖЕННІ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Алгорітм оцінки і управління ризиками при впровадженні корпоративної інформаційної безпеки

3.2. Розробка моделі для оцінки ефективності корпоративної інформаційної безпеки.
3.3. Шляхи покращення ефективності впровадження корпоративних інформаційних систем на ПрАТ «Тернопільський молокозавод»

5. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 1	Горбашевська М.О., к.е.н., доцент	29.02.24	29.02.24
Розділ 2	Горбашевська М.О., к.е.н., доцент	29.02.24	29.02.24
Розділ 3	Горбашевська М.О., к.е.н., доцент	29.02.24	29.02.24

6. Дата видачі завдання_____«29»__лютого__ 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Вибір теми кваліфікації роботи	до 29.02.2024	
2.	Затвердження теми кваліфікаційної роботи та наукового керівника	29.02.2024	
3.	Консультація з науковим керівником	постійно	
4.	Робота з науковою літературою. Визначення плану кваліфікаційної роботи	до 29.02.2024	
5.	Робота над теоретичною частиною кваліфікаційної роботи	29.02.2024-30.05.2024	
6.	Подання на перевірку теоретичної частини кваліфікаційної роботи науковому керівнику	до 30.05.2024	
7.	Переддипломна практика	30.09.2024 - 21.10.2024	
8.	Робота над аналітичною частиною кваліфікаційної роботи	30.09.2024-15.11.2024	
9.	Подання на перевірку аналітичної частини кваліфікаційної роботи науковому керівнику	до 15.11.2024	
10.	Попередній захист кваліфікаційної роботи	19.11.2024	
11.	Подання кваліфікаційної роботи на кафедру	до 05.12.2024	
12.	Захист кваліфікаційної роботи	19.12.2024	

Студент _____ Галишинець Ю.І.
(підпис) (прізвище та ініціали)

Науковий керівник роботи _____ Горбашевська М.О.
(підпис) (прізвище та ініціали)

ЗМІСТ

ВСТУП

Новий етап еволюції інформаційного обміну відзначається активним впровадженням передових інформаційних технологій. Цей період характеризується стрімким розвитком локальних, корпоративних та глобальних мереж, які забезпечують нові можливості, підвищують ефективність і якість процесів обміну інформацією.

Сучасний бізнес значною мірою залежить від інформаційних технологій, що робить корпоративну інформаційну безпеку (КІБ) однією з ключових складових успішної діяльності організацій. У той же час загроза кібератак, витоків даних, несанкціонованого доступу та інших інцидентів постійно зростає. Це обумовлює необхідність впровадження ефективних систем КІБ, які здатні не лише захистити інформаційні активи компанії, але й зменшити ризики, пов'язані з реалізацією цих систем.

Актуальність теми зумовлена такими факторами:

1. Зростанням кібератак: Кількість атак на корпоративні мережі щорічно збільшується. Це ставить компанії перед вибором між суттєвими інвестиціями в КІБ та потенційними втратами, які можуть досягати мільйонів доларів.

2. Регуляторними вимогами: У багатьох країнах посилюється законодавство у сфері захисту даних (наприклад, GDPR в ЄС). Недотримання цих вимог може призвести до значних штрафів та втрати репутації.

3. Складністю інтеграції рішень: Впровадження КІБ часто супроводжується технічними труднощами, які можуть спричинити збої в роботі компанії. Зниження ризиків у цьому контексті допомагає уникнути негативних наслідків.

4. Людським фактором: Велика частина загроз виникає через помилки або недбалість співробітників. Важливою частиною зниження ризиків є підвищення обізнаності персоналу у питаннях КІБ.

5. Фінансовою вразливістю: Інвестиції в КІБ повинні бути збалансованими. Надмірне виділення ресурсів може бути нераціональним, а недостатнє — небезпечним.

Отже, зниження ризиків при впровадженні КІБ є стратегічно важливим завданням, що забезпечує стабільність, стійкість і конкурентоспроможність сучасного бізнесу. Вивчення цієї теми дозволяє не лише забезпечити ефективний захист корпоративної інформації, але й оптимізувати витрати, що особливо важливо в умовах економічної нестабільності.

Важливість та недостатня опрацьованість питань, пов'язаних з аналізом і мінімізацією наслідків ризиків під час впровадження корпоративних інформаційних систем, зумовили актуальність обраної теми магістерської роботи.

Питанням управління ризиками інвестиційних проєктів присвячували свої роботи як зарубіжні, так і вітчизняні вчені, серед яких: Ф. Х. Найт, Д. М. Кейнс, Г. М. Марковіц, Д. Б. Данциг, У. Ф. Шарп, Д. Тобін, С. А. Росс, С. Хьюс, К. Редхед, Л. В. Канторович, А. Н. Колмогоров, Г. Александер, Р. А. Фатхутдінов, А. П. Альгін, Ю. В. Трифонов, Ф. Ф. Юрлов, А. А. Первозванський, В. В. Ковальов, В. Є. Кузнєцов та інші. Проблематику створення автоматизованих інформаційних систем досліджували такі науковці, як Н. Дж. Карр, Д. Саммон, М. Екстром, Х. Бьєрнсон, С. В. Пітеркін, І. А. Оладки, Д. В. Ісаєв, А. В. Шустов, О. А. Славін та інші. Вивченням питань впровадження корпоративних інформаційних систем займалися А. А. Абрамова, Т. Є. Андрєєва, А. І. Афонічкін, С. І. Ашмаріна, Д. В. Єрохіна, Н. Н. Моїсеєв, Е. В. Попов та інші дослідники.Наукові праці вищеназваних авторів внесли значний вклад в розвиток інформаційно-технічних комплексів, проте, питання зниження наслідків ризиків при створенні та впровадженні корпоративних інформаційних систем досліджені недостатньо.

Метою роботи є дослідження та обґрунтування теоретичних і методичних підходів до впровадження корпоративної інформаційної безпеки,

а також розробка практичних рекомендацій для мінімізації ризиків, що супроводжують цей процес.

Основні завдання роботи:

- дослідити природу ризику, визначити його значення та місце в діяльності підприємства, а також у процесі впровадження корпоративної інформаційної системи.

- визначити критерії оцінки ефективності проєктів впровадження КІС і розробити алгоритм побудови ефективного процесу впровадження.

- провести систематизацію та класифікацію корпоративної інформаційної безпеки.

- описати структуру та основний зміст етапів процесу впровадження корпоративних інформаційних систем.

- обґрунтувати вибір критеріїв для оцінювання наслідків ризиків, які виникають під час впровадження інформаційної безпеки у діяльність підприємства.

- розробити алгоритм оцінки та управління ризиками інвестування в проєкти корпоративної інформаційної безпеки.

Предметом дослідження є процеси управління ризиками в контексті впровадження корпоративної інформаційної безпеки.

Об'єктом дослідження є корпоративна інформаційна безпека досліджуємого підприємства.

Методи дослідження включають аналітичний підхід, системний аналіз, статистичні методи, методи збору та обробки даних, а також емпіричні методи та методи факторного аналізу.

Магістерська робота складається з: вступу, трьох розділів, висновків та списку використаних джерел. У тексті роботи міститься 13 таблиць і 13 рисунків. Загальний обсяг роботи 93 сторінки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ ТА ВПРОВАДЖЕННЯ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

1.1. Поняття та класифікація корпоративних інформаційних систем

Роль корпоративних інформаційних систем (КІС) в управлінні компанією за останні роки зазнала значних змін. З розвитком комп'ютерних технологій, програмного забезпечення та методів управління інформацією, змінювався й сам зміст цього поняття. Сучасні КІС уже не обмежуються лише формуванням звітів, а здійснюють облік за одночасними вимогами національних та міжнародних стандартів. Сьогоднішні КІС — це складні інтегровані системи, що включають в себе численні модулі, які відповідають за більшість аспектів діяльності підприємства, охоплюючи всі ключові напрямки його роботи: модуль фінансового управління (автоматизація бухгалтерії, фінансове планування, контроль витрат), модуль управління запасами, модуль обліку складських операцій, система управління персоналом, модуль логістики та збуту, система документообігу, маркетингова підсистема, система управління взаємодією з клієнтами.

З погляду програмних технологій, інформаційні системи (ІС) не є єдиним або навіть кількома програмними комплексами. Вони представлені набором механізмів, методів і алгоритмів, які забезпечують підтримку життєвого циклу інформації. Це включає три основні процеси: обробку даних, управління інформацією та управління знаннями.

Інформаційна система (ІС) — це комплексна інфраструктура підприємства, яка забезпечує управління усіма інформаційними та документальними потоками. Обов'язкові елементи ІС представлені ра нисунку 1.1.

Елементи, представлені на рисунку мають певну характеристику:

- Інформаційна модель — це сукупність правил, структур та алгоритмів, які визначають функціонування ІС. Вона включає в себе всі форми документів,

структуру довідників, бази даних та інші компоненти, що використовуються в системі.

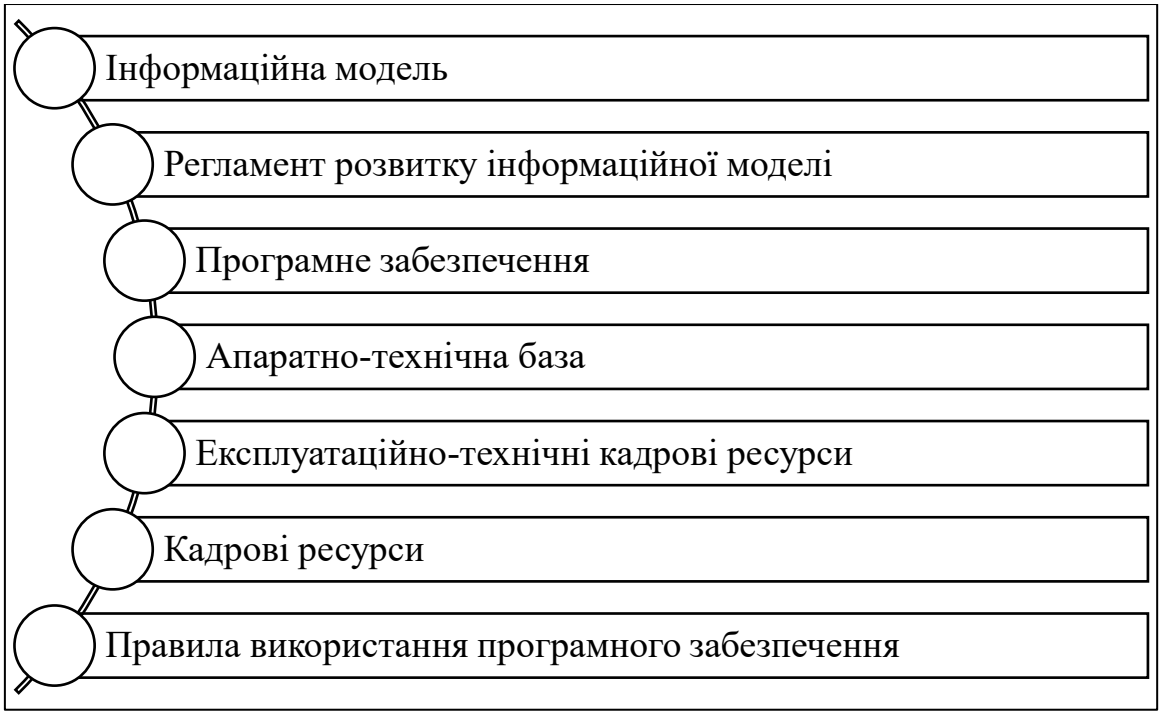

Рисунок 1.1. - Обов'язкові елементи ІС

Джерело: створено автором самостійно

- Регламент розвитку інформаційної моделі — це набір правил, що регулюють процес внесення змін в інформаційну модель та її вдосконалення відповідно до змін у зовнішньому середовищі та внутрішніх вимог підприємства.

- Кадрові ресурси — це команда, яка відповідає за формування та розвиток інформаційної моделі. Це можуть бути співробітники департаменту розвитку ІТ-систем, а також зовнішні консультанти, які мають експертизу в розробці та підтримці ІС.

- Програмне забезпечення — це основний інструмент управління ІС, яке має конфігурацію, що відповідає вимогам інформаційної моделі. Програмне забезпечення не тільки забезпечує виконання операцій, але й служить механізмом для автоматизації управління всіма інформаційними процесами в компанії.

- Кадрові ресурси для налаштування програмного забезпечення — це персонал, який займається адаптацією програмного забезпечення, його

налаштуванням і забезпеченням його відповідності затвердженій інформаційній моделі. Ці спеціалісти відповідають за підтримку системи в актуальному стані.

- Регламент внесення змін — це набір правил, що визначають порядок внесення змін у налаштування, структуру баз даних, а також в конфігурацію програмного забезпечення та його функціональні модулі. Це дозволяє ефективно оновлювати та модернізувати систему в разі потреби.

- Апаратно-технічна база — це обладнання, необхідне для підтримки роботи програмного забезпечення. Включає комп'ютери на робочих місцях, периферійні пристрої, канали зв'язку, системне програмне забезпечення та системи управління базами даних (СУБД), що забезпечують належну роботу ІС.

- Експлуатаційно-технічні кадрові ресурси — це персонал, який займається обслуговуванням та підтримкою апаратно-технічної бази. Вони відповідають за безперебійну роботу технічного обладнання та своєчасне усунення технічних несправностей.

- Правила використання програмного забезпечення — це набір інструкцій, регламентів і політик, які визначають правила роботи користувачів з програмним забезпеченням, а також порядок навчання та сертифікації користувачів. Це допомагає забезпечити належну експлуатацію та безпеку інформаційних систем.

Ця комплексна інфраструктура дозволяє ефективно управляти інформаційними потоками на підприємстві, оптимізувати процеси, підвищувати продуктивність та знижувати ризики.

Ресурси корпорацій поділяються на:

1. Матеріальні ресурси: сировина, готова продукція, основні засоби виробництва.

2. Фінансові ресурси: кошти, фінансові інструменти та інвестиції.

3. Людські ресурси: співробітники та їхній професійний потенціал.

4. Інтелектуальні ресурси: ноу-хау, технології, патенти, інноваційні розробки.

5. Інформаційні ресурси: корпоративні інформаційні системи, бази даних і знання, необхідні для управління та прийняття рішень.

Система управління будь-якої компанії складається з трьох ключових підсистем:

1. Планування продажів і операцій. Ця підсистема формує загальний план діяльності підприємства, визначаючи обсяги виробництва готової продукції. Основний акцент робиться на прогнозуванні попиту та оцінці ресурсів, необхідних для його задоволення. У рамках цієї підсистеми створюється основний виробничий план, який встановлює, які вироби, у якій кількості та в які терміни потрібно виготовити.

2. Детальне планування ресурсів. Цей етап включає точне визначення потреб у матеріалах, виробничих потужностях та трудових ресурсах. Складений план регламентує строки та обсяги замовлень для всіх матеріалів і комплектуючих, необхідних для реалізації основного виробничого плану.

3. Управління виконанням планів. Ця підсистема забезпечує контроль та координацію виконання планів під час виробничого процесу та закупівель. Вона відповідає за своєчасне постачання ресурсів і дотримання графіка виробництва.

Ефективність управління підприємством визначається взаємодією багатьох факторів, серед яких виділяються філософські, історичні, політичні, соціальні, економічні, психологічні, правові, методологічні, організаційні та інформаційно-технологічні аспекти.

Якщо розглядати кожен фактор як інформацію, то інформаційно-технологічний фактор є ключовим. Його реальним проявом або виразом є корпоративні інформаційні системи підприємства.

Корпоративна інформаційна система (КІС) є потужним і гнучким інструментом для формування єдиного інформаційного простору в межах компанії. Вона дозволяє інтегрувати всі інформаційні ресурси та корпоративні

додатки, що сприяє підвищенню ефективності роботи як окремих співробітників, так і підприємства в цілому. Такі системи здатні обробляти великі обсяги даних у реальному часі, що дає змогу оперативно отримувати необхідну інформацію та приймати обґрунтовані рішення. Однією з основних цілей КІС є створення зручного інформаційного середовища, яке полегшує і оптимізує щоденну роботу співробітників, забезпечуючи їм доступ до актуальних даних та автоматизуючи багато рутинних процесів. Це дозволяє підвищити продуктивність, зменшити ймовірність помилок та зробити бізнес-процеси більш ефективними [3, с.25].

Корпоративна інформаційна система (КІС) — це набір методів та рішень, що застосовуються для формування єдиного інформаційного простору управління та підтримки функціонування компанії [5].

Основне завдання КІС — забезпечення ефективного управління всіма ресурсами підприємства (матеріальними, фінансовими, технологічними та інтелектуальними) з метою досягнення максимального прибутку та задоволення матеріальних і професійних потреб співробітників компанії.

Корпоративна інформаційна система (КІС) є комплексом різноманітних програмно-апаратних платформ, універсальних та спеціалізованих додатків від різних розробників, інтегрованих в єдину, інформаційно однорідну систему. Вона розробляється таким чином, щоб максимально ефективно вирішувати унікальні завдання, властиві кожному конкретному підприємству. КІС є людино-машинною системою, яка служить інструментом підтримки інтелектуальної діяльності співробітників. Завдяки такій системі, підприємство здатне:

- Накопичувати досвід та формалізовані знання, що використовуються для прийняття рішень і підвищення ефективності роботи.

- Постійно вдосконалюватися та розвиватися, адаптуючи свої функції до змінюваних умов.

- Швидко реагувати на зміни в зовнішньому середовищі та нові потреби підприємства, що дозволяє оперативно коригувати стратегію та бізнес-процеси.

Таким чином, КІС не тільки автоматизує процеси, а й стає гнучким інструментом для постійного розвитку та адаптації організації до нових викликів.

Комплексна автоматизація підприємства передбачає переведення всіх основних бізнес-процесів організації в сферу комп'ютерних технологій. Використання спеціалізованого програмного забезпечення, яке забезпечує інформаційну підтримку бізнес-процесів, є найефективнішим і доцільним підходом для створення КІС. Сучасні системи управління бізнес-процесами дозволяють інтегрувати різні програмні продукти в єдину інформаційну систему. Це дозволяє вирішити проблеми координації діяльності співробітників і підрозділів, забезпечити їх необхідною інформацією та контролювати виконання завдань, при цьому керівництво має можливість отримувати своєчасний доступ до достовірних даних про хід виробничих процесів і приймати оперативні управлінські рішення. Що важливо, автоматизована система є гнучкою та відкритою, що дає змогу легко адаптувати її до змін і доповнювати новими модулями або зовнішнім програмним забезпеченням за необхідності.

Під корпоративною інформаційною системою розуміється інформаційна система організації, яка відповідає мінімальним вимогам, зокрема:

1. Функціональна повнота — система повинна забезпечувати виконання всіх необхідних функцій для підтримки діяльності організації.

2. Надійність захисту інформації — система повинна включати ефективні механізми для захисту даних від несанкціонованого доступу та втрат.

3. Інструменти адаптації та супроводу — система має бути оснащена засобами для її налаштування та підтримки в актуальному стані.

4. Підтримка віддаленого доступу та роботи в розподілених мережах — можливість доступу до системи з різних локацій і роботи в мережах, що охоплюють кілька географічних точок.

5. Обмін даними між різними інформаційними системами та програмними продуктами — система повинна забезпечувати ефективний обмін інформацією між різними внутрішніми і зовнішніми системами.

6. Консолідація інформації — можливість централізованого збору і обробки даних з різних джерел для формування єдиного інформаційного потоку.

7. Спеціалізовані засоби аналізу стану системи — наявність інструментів для моніторингу та аналізу ефективності та стабільності роботи системи під час її експлуатації.

Найбільш розвинені корпоративні інформаційні системи (КІС) призначені для автоматизації всіх управлінських функцій корпорації: від науково-технічної та маркетингової підготовки до реалізації продукції та послуг. На сьогодні більшість КІС орієнтовані переважно на економічні та виробничі аспекти діяльності підприємства.

При розробці класифікації КІС ми проаналізуємо корпоративні інформаційні системи, які були виділені в процесі дослідження ринку інформаційно-технічних послуг. Ми також надамо орієнтовну вартість таких систем, варіанти захисту інформації, визначимо їх цілі, основні функції та приблизні терміни впровадження.

Класифікація інформаційних систем, яка представлена в таблиці 1.1. може здійснюватися за різними критеріями, що залежать від мети, яку ставить перед собою аналітик. Однією з основних ознак для оцінки систем з точки зору їх розвитку є ступінь інтеграції інформації. За цією ознакою можна виділити чотири основні групи.

Таблиця 1.1.

Класифікація інформаційних систем

Критерії класифікації	Основні види
Ступінь інтеграції	Локальні системи
	Малі інтегровані системи
	Середні інтегровані системи
	Великі інтегровані системи
Види автоматизованих бізнес-процесів	Об'ємно-календарне планування (MPS)
	Планування потреби в матеріалах (MRP)
	Управління ланцюжками поставок (SCM)
	Планування фінансових ресурсів (FRP)
	Планування виробничих ресурсів (CRP)
	Обслуговування клієнтів організацій (CRM)
	Планування виробництва (MRPII)
	Планування ресурсів підприємства (ERP)
	Планування ресурсів, синхронізоване зі споживачем (CSRP)
Спосіб впровадження	Адаптивні системи
	Унікальні (замовні) системи
Вартість впровадження	Локальні системи
	Фінансово-управлінські системи
	Середні інтегровані системи
	Великі інтегровані системи

Джерело: створено автором самостійно

Розглянемо їх більш детально:

1. Локальні системи — це, як правило, облікові системи, що функціонують на рівні окремих підрозділів або для специфічних завдань, наприклад, бухгалтерського обліку або управління персоналом.

2. Малі інтегровані системи — комплексні рішення для обліку та управління, зокрема в галузі фінансів, що поєднують різні аспекти управлінських процесів у межах окремих функціональних підсистем підприємства.

3. Середні інтегровані системи — ці системи охоплюють більший масштаб діяльності підприємства і можуть забезпечувати комплексне управління на рівні середніх організацій або окремих підрозділів, включаючи фінанси, виробництво та інші функції.

4. Великі інтегровані системи — системи, які забезпечують комплексне управління для великих підприємств з широким масштабом виробництва.

Вони інтегрують всі функції компанії, включаючи фінансове управління, виробничі процеси, логістику, маркетинг та інші важливі аспекти діяльності.

Ця класифікація дозволяє чітко визначити рівень інтеграції системи в рамках підприємства та її здатність покривати різні аспекти управління в залежності від розміру та складності бізнес-процесів.

За способом впровадження існують два основні типи корпоративних інформаційних систем (КІС):

1. Адаптивні системи, які базуються на наборі типових бізнес-процесів. Вони розроблені так, щоб їх можна було адаптувати під потреби різних підприємств, зокрема шляхом налаштування під конкретні умови та вимоги організації.

2. Унікальні (замовні) системи, які орієнтовані на конкретні корпорації та їхні організаційно-економічні особливості. Такі системи створюються з урахуванням специфічних потреб та процесів компанії і часто потребують індивідуального підходу до розробки та впровадження [6].

Ці два типи систем мають різний підхід до впровадження та налаштування, при цьому адаптивні системи зазвичай дешевші і швидше впроваджуються, тоді як унікальні системи забезпечують гнучкість та максимальну відповідність вимогам конкретної організації.

За вартістю впровадження корпоративні інформаційні системи (КІС) можна поділити на чотири основні категорії:

1. Локальні системи — найбільш доступні за вартістю, ці системи автоматизують облік в окремих функціональних областях, таких як бухгалтерія, складський облік, податковий облік тощо. Вони зазвичай застосовуються для невеликих підприємств або окремих підрозділів великих компаній.

2. Фінансово-управлінські системи — ці системи забезпечують автоматизацію фінансових та управлінських процесів, таких як планування бюджету, управління грошовими потоками, аналіз фінансових показників.

Вартість їх впровадження вище за локальні системи, але вони мають більш широку функціональність, що дозволяє ефективно управляти підприємством.

3. Середні інтегровані системи — ці системи охоплюють більший масштаб діяльності підприємства, інтегруючи різні функції, такі як фінанси, виробництво, постачання та інші аспекти бізнесу. Вартість таких систем є середньою, і вони підходять для середніх за розміром організацій.

4. Великі інтегровані системи — ці системи забезпечують комплексне управління для великих підприємств, інтегруючи всі функціональні області і підтримуючи складні бізнес-процеси на підприємствах з великим масштабом виробництва. Вартість впровадження таких систем є найвищою через їхню складність і потребу в спеціалізованому підході до налаштування та інтеграції.

Ця класифікація допомагає зрозуміти, який тип системи найбільше відповідає потребам підприємства, залежно від його розміру, складності процесів та бюджету на впровадження.

За видами автоматизованих бізнес-процесів корпоративні інформаційні системи (КІС) можна класифікувати відповідно до методологій, що лежать в їх основі. Кожна методологія спрямована на оптимізацію конкретних аспектів управління підприємством [12]:

1. Об'ємно-календарне планування (MPS) — використовується для планування обсягів виробництва, що базується на встановлених часових рамках та обсягах замовлень.

2. Планування потреби в матеріалах (MRP) — орієнтоване на визначення необхідної кількості матеріалів та комплектуючих для забезпечення виробничого процесу.

3. Управління ланцюжками поставок (SCM) — фокусується на оптимізації всіх етапів ланцюга поставок, від постачальників до кінцевих споживачів.

4. Планування фінансових ресурсів (FRP) — направлене на управління фінансовими потоками компанії, зокрема на бюджетування, планування витрат і доходів.

5. Планування виробничих ресурсів (CRP) — спрямоване на ефективне управління виробничими потужностями, персоналом і іншими ресурсами в процесі виробництва.

6. Обслуговування клієнтів організацій (CRM) — зосереджується на управлінні взаємовідносинами з клієнтами, забезпечуючи ефективне обслуговування та підтримку.

7. Планування виробництва (MRPII) — інтегрує планування виробничих процесів з іншими функціями, такими як закупівля, складування, та управління запасами.

8. Планування ресурсів підприємства (ERP) — є комплексною методологією, яка інтегрує всі ресурси підприємства (фінансові, людські, матеріальні) для досягнення максимального ефекту.

9. Планування ресурсів, синхронізоване зі споживачем (CSRP) — фокусується на злагодженому плануванні та управлінні ресурсами відповідно до потреб кінцевих споживачів та вимог ринку.

Ці методології дозволяють підприємствам більш ефективно управляти своїми бізнес-процесами, оптимізуючи витрати, покращуючи якість обслуговування та підвищуючи загальну ефективність роботи.

За словами деяких дослідників, планування заходів для мінімізації наслідків ризиків у корпоративних інформаційних системах (КІС), впровадження яких займає менше одного року, є малоефективним. Зазвичай, функціонал таких систем є базовим для відповідної галузі організації. Однак винятками є унікальні КІС та ті, що використовують новітні технології [2,3,6,12].

Аналіз корпоративних інформаційних систем (КІС) показав, що найбільший інтерес для процесу управління ризиками представляють фінансово-управлінські системи з терміном впровадження більше року, а також середні та великі інтегровані КІС, які автоматизують кілька бізнес-процесів організації одночасно. До цієї категорії належать як адаптивні системи, що базуються на стандартних бізнес-процесах, так і унікальні КІС,

розроблені для конкретних потреб підприємства. Такі системи дозволяють більш ефективно оцінювати і управляти ризиками завдяки інтеграції різних аспектів управлінської та виробничої діяльності організації, що дає змогу оперативно реагувати на зміни та мінімізувати потенційні негативні наслідки.

1.2 Корпоративна інформаційна безпека: її характеристика та складові

Корпоративна інформаційна безпека (КІБ) є важливим аспектом сучасного корпоративного управління та управління ризиками. З розвитком цифрових технологій, зростанням обсягів даних і залежності бізнесу від інформаційних систем, питання захисту інформації набуває критичного значення для забезпечення стабільного функціонування підприємств, їхньої конкурентоспроможності та репутації.

Корпоративна інформаційна безпека – це сукупність політик, процедур, технологій і заходів, спрямованих на захист інформаційних активів організації від несанкціонованого доступу, використання, модифікації, розголошення чи знищення. Вона включає як технічні, так і організаційні аспекти забезпечення конфіденційності, цілісності та доступності інформації.

Основні елементи корпоративної інформаційної безпеки представлені на рисунку 1.2.

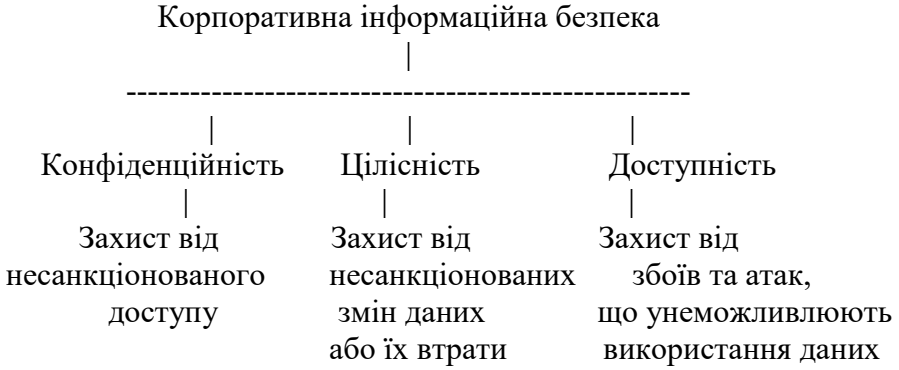

Рисунок 1.2. – Схема основних елементів корпоративної інформаційної безпеки

Джерело: створено автором самостійно

Як бачимо з рисунку є три основних елемента корпоративної інформаційної безпеки:

1. **Конфіденційність** – забезпечення доступу до інформації лише уповноваженим особам.

2. **Цілісність** – гарантія того, що дані не будуть змінені або знищені без відповідного дозволу.

3. **Доступність** – забезпечення можливості використання інформації тоді, коли вона потрібна.

Основні елементи системи безпеки тісно пов’язані з ключовими аспектами корпоративної інформаційної безпеки. Кожен з елементів сприяє зміцненню одного або кількох аспектів безпеки, забезпечуючи їх інтеграцію та ефективність. У результаті цього створюється стійка система, яка гарантує захист інформаційних активів і підтримує функціонування організації на високому рівні безпеки. Ключові аспекти корпоративної інформаційної системи представлені в таблиці 1.2.

Таблиця 1.2.

Ключові аспекти корпоративної інформаційної системи

Аспект	Характеристика	Приклади заходів
Правові та нормативні вимоги	Забезпечення відповідності законам та стандартам	Виконання вимог GDPR, ISO 27001, законодавства України про захист персональних даних.
Організаційні заходи	Створення внутрішніх політик та процесів	Політика безпеки, інструкції для співробітників, навчальні програми.
Технічні заходи	Використання програмного забезпечення та технологій	Шифрування даних, брандмауери, антивірусні системи, моніторинг мереж.
Управління ризиками	Аналіз і зниження загроз	Оцінка ризиків, впровадження планів реагування на інциденти, резервне копіювання даних.
Психологічні аспекти	Формування культури інформаційної безпеки	Регулярні тренінги, мотивація співробітників, контроль над людським фактором.

Джерело: створено автором

Як бачимо у таблиці наведено ключові аспекти корпоративної інформаційної безпеки (КІБ), які охоплюють правові, організаційні, технічні, управлінські та психологічні заходи. Розглянем їх більш детально:

1. Правові та нормативні вимоги. Цей аспект зосереджується на забезпеченні відповідності організації всім необхідним законам, стандартам та нормативним актам, що регулюють сферу інформаційної безпеки. Виконання цих вимог є обов'язковим для уникнення юридичних санкцій та захисту прав компанії і її клієнтів.

- Виконання вимог GDPR (Загальний регламент захисту даних Європейського Союзу): забезпечення обробки персональних даних відповідно до вимог щодо збереження конфіденційності та права на доступ до особистих даних.

- ISO 27001: сертифікація системи управління інформаційною безпекою, що включає політики, процедури та контрольні заходи для забезпечення безпеки даних.

- Законодавство України про захист персональних даних: виконання положень Закону України "Про захист персональних даних", яке передбачає правила обробки, зберігання та передачі персональних даних.

2. Організаційні заходи включають створення та впровадження внутрішніх політик, процедур та стандартів, які регулюють інформаційну безпеку в організації. Вони визначають, як має бути організовано управління інформаційною безпекою на рівні організації.

- Політика безпеки: Визначення основних принципів і правил щодо захисту інформаційних активів, доступу до даних і користувацьких прав.

- Інструкції для співробітників: Документація, що пояснює співробітникам правила безпеки, процедури щодо роботи з конфіденційною інформацією, використання корпоративних ресурсів.

- Навчальні програми: Регулярне навчання персоналу щодо сучасних загроз інформаційній безпеці, правил роботи з даними та способів запобігання інцидентам.

3. Технічні заходи включають використання програмних та апаратних засобів для забезпечення інформаційної безпеки. Ці заходи націлені на автоматизацію захисту даних і систем від зовнішніх і внутрішніх загроз.

- Шифрування даних: Використання криптографічних методів для захисту даних від несанкціонованого доступу під час їх передачі або зберігання.

- Брандмауери (Firewall): Захист корпоративних мереж від несанкціонованого доступу, відстеження і блокування потенційно небезпечних з'єднань.

- Антивірусні системи: Виявлення та блокування шкідливих програм, таких як віруси, трояни, програмне забезпечення для шпигунства, що можуть пошкодити або викрасти дані.

- Моніторинг мереж: Постійне спостереження за станом мережі для виявлення аномальної активності, що може свідчити про вторгнення або інші загрози.

4. Управління ризиками – це оцінка, аналіз і зниження можливих загроз і вразливостей у системі корпоративної інформаційної безпеки. Включає оцінку можливих наслідків і ймовірностей різних загроз і впровадження заходів для їх нейтралізації.

- Оцінка ризиків: Процес виявлення і оцінки потенційних загроз і вразливостей в системах і процесах організації.

- Впровадження планів реагування на інциденти: Розробка процедур для швидкого реагування на інциденти безпеки (вторгнення, витік даних, збої в роботі систем).

- Резервне копіювання даних: Регулярне створення резервних копій даних, щоб у разі втрати або пошкодження інформації її можна було швидко відновити.

5. Психологічні аспекти врахування людського фактору при забезпеченні інформаційної безпеки. Це важливий аспект, оскільки більшість загроз може бути викликана помилками або недбалістю співробітників.

- Регулярні тренінги: Підвищення обізнаності співробітників щодо сучасних загроз, таких як фішинг, соціальна інженерія, або маніпуляції.

- Мотивація співробітників: Створення стимулів для співробітників до дотримання політики безпеки, наприклад, нагороди за ініціативу щодо безпеки або виявлення вразливостей.

- Контроль над людським фактором: Аналіз та мінімізація помилок користувачів через автоматизацію деяких процесів та навчання.

Забезпечення корпоративної інформаційної безпеки — це багатоаспектний процес, який вимагає комплексного підходу та інтеграції різних заходів. Правові та нормативні вимоги гарантують відповідність закону, організаційні заходи забезпечують чітку стратегію та політику безпеки, технічні заходи пропонують ефективні інструменти захисту, а управління ризиками дозволяє прогнозувати та реагувати на загрози. Психологічні аспекти сприяють формуванню культури безпеки серед співробітників. Тільки завдяки інтеграції всіх цих аспектів можна створити ефективну та стійку систему корпоративної інформаційної безпеки.

Корпоративна інформаційна безпека стикається з безліччю викликів (рис.1.3.), які стають все більш актуальними з розвитком технологій та зміною умов ведення бізнесу. Основні виклики, які потребують особливої уваги для захисту інформаційних ресурсів організацій, включають зростання кількості кібератак, зміни в організаційних структурах через віддалену роботу, інтеграцію нових технологій, таких як хмара, та проблему людського фактору.

Рисунок 1.3. – Виклики корпоративної інформаційної системи

Джерело: створено автором

Розглянемо ці виклики детальніше.

1. Зростання кількості кібератак і загроз

З кожним роком кількість і складність кібератак на організації зростають. Технології, що використовуються для здійснення атак, постійно удосконалюються, і це ставить перед компаніями серйозні завдання щодо захисту своїх даних і систем.

Типи загроз, що зростають:

- Фішинг: Це атаки, що використовують соціальну інженерію для обману співробітників або користувачів з метою отримання конфіденційної інформації, такої як паролі або фінансові дані. Часто ці атаки виглядають як легітимні повідомлення від банків, партнерів або компанії.

- Атаки програм-вимагачів (Ransomware): Вони спричиняють шифрування важливих даних і вимагають викуп для їх відновлення. Ці атаки можуть призвести до серйозних фінансових втрат і пошкодження репутації компанії. Наприклад, атаки на медичні установи або органи державної влади, що паралізують роботу і вимагають мільйонних виплат.

- DDoS-атаки (розподілені атаки на відмову в обслуговуванні): Метою таких атак є перевантаження серверів або мереж компанії величезною кількістю запитів, що призводить до їх недоступності для легітимних користувачів. Це може мати серйозні наслідки для бізнесу, особливо для компаній, які залежні від онлайн-сервісів.

Виклики:

- Підвищення складності атак та їх різноманіття.

- Постійне оновлення методів захисту для боротьби з новими загрозами.

- Зростаюча вартість кіберстрахування через зростання ризиків.

2. Розширення меж корпоративних мереж через використання віддаленої роботи

Віддалена робота стала масовим трендом, і вона значно змінила ландшафт корпоративної безпеки. Тепер співробітники можуть працювати з різних локацій, що ставить перед організацією нові виклики в забезпеченні доступу до корпоративних ресурсів та захисту даних.

Проблеми:

- Невизначеність безпеки підключень: Віддалені працівники використовують домашні мережі, що не завжди мають високий рівень захисту. Це збільшує ризик того, що зловмисники можуть отримати несанкціонований доступ до корпоративних даних.

- Використання незахищених пристроїв: Співробітники можуть підключати свої особисті пристрої до корпоративних мереж, що може створити додаткові вразливості (наприклад, відсутність оновлень безпеки на мобільних пристроях).

- Відсутність фізичного контролю: При роботі на відстані немає можливості безпосередньо контролювати доступ до серверів і робочих місць, що підвищує ризик витоку інформації.

Виклики:

- Забезпечення надійних VPN-з’єднань для віддалених працівників.

- Інтеграція системи управління доступом, щоб переконатися, що тільки уповноважені користувачі можуть отримати доступ до чутливої інформації.

- Навчання співробітників щодо використання безпечних каналів зв’язку та захисту особистих пристроїв.

3. Інтеграція хмарних технологій

З розвитком технологій все більше компаній обирають хмарні рішення для зберігання даних і обробки інформації. Хмара забезпечує гнучкість і масштабованість, але разом з тим створює нові ризики для безпеки, оскільки дані передаються через мережу і зберігаються на серверах, які можуть бути розташовані в різних регіонах або навіть країнах.

Проблеми:

- Контроль за даними: Переміщення даних у хмару вимагає ретельного контролю доступу та моніторингу за їх використанням. Оскільки сервери можуть бути розташовані за межами країни, можуть виникнути питання щодо відповідності міжнародним стандартам безпеки та законодавству.

- Відповідальність за безпеку: Питання, хто несе відповідальність за збереження даних — постачальник хмарних послуг чи сам користувач, стає все більш важливим. Без належного контролю з боку організації існує ризик витоку або втрати даних.

- Доступність і резервне копіювання: Потрібно впровадити політики і технології, що забезпечують надійне резервне копіювання даних у хмарі для запобігання їх втраті.

Виклики:

- Забезпечення безпечної передачі та зберігання даних.

- Перевірка відповідності хмарних постачальників вимогам безпеки та стандартам.

- Захист даних у процесі переміщення між різними хмарними середовищами.

4. Людський фактор (помилки працівників, свідомі порушення)

Людський фактор залишається одним з найбільших викликів у сфері інформаційної безпеки. Більшість загроз виникає через помилки або порушення з боку співробітників. Це можуть бути як випадкові помилки, так і свідомі порушення політик безпеки.

Проблеми:

- Незнання або недбалість: Співробітники можуть не знати або ігнорувати важливі політики безпеки, що веде до несанкціонованого доступу або витоку інформації.

- Фішинг та соціальна інженерія: Атаки, спрямовані на психологічний вплив на працівників, з метою отримання доступу до корпоративних даних.

- Свідомі порушення: У деяких випадках співробітники можуть свідомо порушувати політики безпеки, наприклад, для власної вигоди (наприклад, продажу конфіденційних даних або допомоги конкурентам).

Виклики:

- Виявлення та запобігання свідомим порушенням з боку співробітників.

- Навчання персоналу та підвищення його обізнаності щодо важливості інформаційної безпеки.

- Впровадження технологій для моніторингу та виявлення підозрілої активності в системах, що може вказувати на порушення політики безпеки.

Корпоративна інформаційна безпека стикається з численними викликами, які постійно змінюються залежно від технологічних інновацій, змін у робочих процесах і розвитку кіберзагроз. Зростання кількості кібератак, зокрема фішингу, програм-вимагачів та DDoS-атак, вимагає постійної адаптації захисних заходів. Розширення корпоративних мереж через віддалену роботу та інтеграцію хмарних технологій додає нові ризики, пов'язані з доступом і зберіганням даних. Однак, незважаючи на технічні та організаційні заходи, людський фактор залишається найбільшим викликом для забезпечення безпеки. Навчання та мотивація співробітників до дотримання політик безпеки, а також моніторинг їх поведінки, стають ключовими елементами в побудові ефективної системи зах

Корпоративна інформаційна безпека є невід'ємною складовою сучасної стратегії управління будь-якою організацією, оскільки вона має прямий вплив на безпеку, ефективність та репутацію компанії. Ефективна система корпоративної інформаційної безпеки не лише захищає від зовнішніх і внутрішніх загроз, але й підтримує стабільний розвиток компанії в умовах цифровізації та швидко змінюваного бізнес-середовища. В таблиці 1.3. представлено значення основних аспектів корпоративної інформаційної безпеки.

Таблиця 1.3.

Основні аспекти корпоративної інформаційної безпеки

Основні аспекти	Характеристика	Важливість
Захист репутації компанії	Захист інформації від загроз, що можуть зашкодити іміджу компанії, включаючи витік даних та інші інциденти безпеки.	Втрата довіри до компанії може призвести до зменшення кількості клієнтів, падіння продажів та втрати партнерів.
Мінімізація фінансових втрат	Запобігання фінансовим втратам через інциденти безпеки, такі як штрафи, витрати на відновлення та компенсації.	Зниження витрат на відновлення після інцидентів допомагає компанії зберегти фінансову стабільність.
Виконання законодавчих вимог	Дотримання національних і міжнародних стандартів та законів про захист даних, що дозволяє уникнути юридичних санкцій.	Порушення законодавства може призвести до великих штрафів і юридичних наслідків.
Підвищення довіри клієнтів та партнерів	Формування довіри через забезпечення надійного захисту даних клієнтів та партнерів, виконання стандартів безпеки.	Високий рівень безпеки допомагає залучати нових клієнтів та партнерів, зміцнюючи довіру і стимулюючи розвиток бізнесу.

Джерело: створено автором

1. Захист репутації компанії

Корпоративна репутація є одним з найбільших активів компанії, і будь-яка інформаційна загроза чи інцидент може значно пошкодити її імідж. У разі витоку або порушення даних (наприклад, через кібератаку чи людську помилку) клієнти та партнери можуть втратити довіру до компанії. Репутаційні ризики виникають також через невиконання стандартів безпеки,

що може призвести до негативної публічності та сприйняття компанії як ненадійного партнера.

Важливість:

- Втрата довіри до компанії може призвести до зменшення кількості клієнтів, падіння продажів або втрати стратегічних партнерів.

- Пошкоджена репутація може вимагати значних витрат на відновлення бренду, а також негативно впливати на ринкову вартість компанії.

Кіберінцидент у великій фінансовій установі, що призвів до витоку персональних даних клієнтів, може зашкодити іміджу компанії, навіть якщо інцидент не спричинив безпосередніх фінансових збитків.

2. Мінімізація фінансових втрат у разі інцидентів

Інциденти безпеки можуть призвести до значних фінансових втрат для компанії. Це можуть бути як прямі витрати, такі як штрафи, витрати на відновлення даних і систем, так і непрямі витрати, пов'язані з відновленням репутації або втратою клієнтів.

Важливість:

- Захист корпоративних даних і мереж допомагає знизити ймовірність великих витрат на відновлення після інциденту, таких як витрати на юридичні послуги, штрафи або відшкодування збитків постраждалим сторонам.

- Захист від кібератак дозволяє зменшити витрати на відновлення, що значно скорочує можливі фінансові втрати для компанії.

Атака програмою-вимагачем (ransomware) може призвести до втрати доступу до важливих корпоративних даних і систем, що може спричинити величезні витрати на їх відновлення та компенсацію збитків.

3. Виконання законодавчих вимог

Корпоративна інформаційна безпека також передбачає виконання національних і міжнародних стандартів і законодавчих вимог, спрямованих на захист персональних даних і безпеку інформації. Це є важливим аспектом, оскільки порушення вимог може призвести до юридичних санкцій, штрафів або навіть судових позовів.

Важливість:

- Порушення законодавства про захист даних (наприклад, GDPR у ЄС або закони про захист персональних даних в Україні) може призвести до величезних штрафів і санкцій, які можуть значно вплинути на фінансову стабільність компанії.

- Дотримання стандартів безпеки дозволяє організації уникнути юридичних проблем і підтримувати позитивний імідж у співпраці з державними органами та іншими партнерами.

Недотримання вимог GDPR щодо захисту персональних даних може призвести до штрафів на суму до 4% річного обороту компанії або 20 мільйонів євро (вибирається більша сума).

4. Підвищення довіри клієнтів та партнерів

Інформаційна безпека є критично важливою для створення довіри серед клієнтів і бізнес-партнерів. Організації, які мають надійні системи захисту інформації, демонструють свою відповідальність і професіоналізм, що стимулює розвиток партнерських відносин і залучення нових клієнтів.

Важливість:

- Клієнти та партнери хочуть бути впевненими, що їхні дані та інформація знаходяться під належним захистом, і що компанія готова реагувати на будь-які загрози.

- Наявність сертифікацій та виконання міжнародних стандартів безпеки може служити додатковим фактором при виборі постачальника послуг або партнера.

Компанія, що володіє сертифікацією ISO 27001 або іншими стандартами безпеки, має конкурентну перевагу, оскільки її партнери та клієнти можуть бути впевнені, що їхні дані знаходяться під надійним захистом.

Корпоративна інформаційна безпека має ключове значення для захисту репутації компанії, мінімізації фінансових втрат, виконання законодавчих вимог і підвищення довіри клієнтів та партнерів. Без належного рівня захисту інформації організація ризикує втратити клієнтів, понести значні фінансові

витрати через інциденти безпеки або навіть зіткнутися з юридичними наслідками. Встановлення ефективної системи корпоративної інформаційної безпеки є необхідною умовою для забезпечення стабільності, розвитку та успіху компанії в умовах сучасного цифрового середовища.

1.3 Характеристика ризиків інформаційної безпеки в корпоративній інформаційній системі

Ризик присутній практично у всіх аспектах людської діяльності, тому його точне та універсальне визначення сформулювати складно. У підприємницькій діяльності ризик має самостійне теоретичне та прикладне значення, виступаючи невід'ємною складовою теорії та практики управління.

Термін «ризик» набуває конкретного значення та інтерпретації лише в контексті певних видів діяльності та типів ризиків. Таким чином, класифікація ризиків має здійснюватися з урахуванням визначених цілей і завдань.

Ризик інформаційної безпеки визначається як ймовірність виникнення несприятливої події внаслідок реалізації загроз, спрямованих на вразливі інформаційні ресурси, з урахуванням можливих негативних наслідків [12].

Сучасна діяльність фірми немислима без ефективно функціонуючої корпоративної інформаційної системи, яка забезпечує безперервний обмін діловою інформацією незалежно від місця перебування користувачів. Така система є ключовим інструментом для підтримки оперативності, взаємодії та продуктивності в бізнес-процесах.

Забезпечення безпеки діяльності фірми, у широкому сенсі, реалізується через створення комплексної системи захисту. Ця система являє собою ретельно розроблений набір заходів, технологій та інструментів, спрямованих на виявлення, попередження та нейтралізацію потенційних загроз, які можуть вплинути на стабільність і безпеку діяльності компанії.

Кожен об'єкт захисту, чи то бізнес-процес, інформаційний ресурс, чи технічний засіб, має свої унікальні характеристики та вразливості. Ці особливості повинні бути враховані при формуванні загальної стратегії

безпеки. Це означає, що система захисту повинна бути гнучкою, адаптивною та здатною враховувати специфіку кожного елемента. Наприклад:

- процеси потребують захисту від збоїв та несанкціонованих втручань.

- технічні засоби мають бути оснащені сучасними засобами захисту від кібератак та фізичних пошкоджень.

- інформаційні ресурси повинні бути захищені від втрат, несанкціонованого доступу або витоку даних.

У сучасних умовах розвитку технологій і глобалізації бізнесу, система безпеки фірми повинна інтегрувати інноваційні підходи, такі як використання штучного інтелекту для моніторингу загроз, впровадження багаторівневої аутентифікації, шифрування даних, а також регулярне навчання персоналу основам інформаційної безпеки. Лише такий комплексний підхід дозволить забезпечити ефективний захист і стабільність діяльності компанії.

Спотворення інформації, важливої для ухвалення ключових бізнес-рішень, блокування доступу до неї від партнерів або співробітників, поширення неправдивих даних, а також знищення існуючих ресурсів, що містять фінансову, маркетингову або технологічну інформацію, можуть завдати серйозної шкоди діловій репутації компанії. Це здатне призвести до прийняття невірних рішень, наслідком яких стають значні матеріальні втрати та інші негативні наслідки для бізнесу.

Інформація, яка обробляється в корпоративних інформаційних системах, має підвищений рівень вразливості. Це пов’язано з ризиком несанкціонованого доступу, модифікації даних або впровадження неправдивої інформації, що може завдати серйозної шкоди бізнесу. Сучасні технологічні умови значно посилюють ці ризики через такі фактори:

- Зростання обсягів інформації: постійне збільшення кількості даних, які передаються і зберігаються в корпоративних комп'ютерних системах, створює більше точок доступу для потенційних зловмисників.

- Концентрація важливих даних: бази даних містять інформацію різного рівня важливості й конфіденційності, включаючи фінансові, маркетингові, технічні та комерційні дані, що робить їх привабливою ціллю для атак.

- Розширення доступу: зростання кількості користувачів, які мають доступ до баз даних і ресурсів корпоративних обчислювальних мереж, підвищує ймовірність витоків або неправомірного використання інформації.

- Збільшення віддалених робочих місць: популяризація дистанційної роботи ускладнює контроль доступу, створюючи додаткові вразливості для корпоративної системи.

- Використання глобальних мереж: інтеграція глобальної мережі Internet і різноманітних каналів зв'язку для передачі даних значно розширює можливості несанкціонованого втручання.

- Автоматизація обміну даними: автоматичний обмін інформацією між комп'ютерами користувачів підвищує швидкість передачі даних, але водночас збільшує ризик поширення помилкової або шкідливої інформації.

Зазначені фактори посилюються низьким рівнем захищеності систем, застарілими засобами кіберзахисту, а також браком обізнаності працівників щодо основ інформаційної безпеки. Зростання залежності компаній від інформаційних систем підкреслює необхідність впровадження комплексних заходів для захисту корпоративних даних (рис.1.4.).

До таких заходів належать:

1. Контроль доступу: впровадження багаторівневої аутентифікації, обмеження доступу до конфіденційних даних та моніторинг активності користувачів.

2. Шифрування даних: забезпечення надійного шифрування інформації, що передається або зберігається.

3. Регулярне оновлення систем: своєчасне оновлення програмного забезпечення та виправлення вразливостей.

Рисунок 1.4. – Комплексні заходи до захисту корпоративних даних

Джерело: створено автором

4. Навчання персоналу: організація тренінгів з кібербезпеки для всіх співробітників.

5. Інтеграція засобів моніторингу: впровадження систем для виявлення аномалій у мережевому трафіку та поведінці користувачів.

Ефективний захист інформації в корпоративних системах потребує поєднання технологічних, організаційних і освітніх заходів, які дозволять мінімізувати ризики й забезпечити стабільну роботу компанії.

Ризики інформаційної безпеки в корпоративній інформаційній системі є багатогранними та охоплюють різні аспекти діяльності організації. Їх характеристика включає визначення джерел загроз, механізмів впливу та можливих наслідків. Основні види ризиків можна класифікувати за такими категоріями:

1. Технічні ризики:

- вразливості програмного забезпечення: недоліки в коді або конфігурації, які можуть бути використані для атак.

- збої обладнання: відмова серверів, мережевих пристроїв або систем зберігання даних.

- атаки на мережі: DDoS-атаки, перехоплення даних, злом мережевих протоколів.

2. Організаційні ризики:

- відсутність політики інформаційної безпеки: відсутність документованих правил та регламентів.

- недостатній контроль доступу: слабкі паролі, відсутність багаторівневої аутентифікації.

- недбалість співробітників: порушення процедур безпеки через необізнаність або нехтування вимогами.

3. Зовнішні загрози:

- кібератаки: хакерські зломи, впровадження шкідливого ПЗ, фішинг.

- соціальна інженерія: маніпуляції для отримання конфіденційної інформації.

- фізичні загрози: крадіжка обладнання або несанкціонований фізичний доступ до систем.

4. Внутрішні загрози:

- шкідливі дії співробітників: зловживання доступом або навмисне пошкодження даних.

- випадкові помилки: видалення або розголошення даних через недбалість.

5. Ризики пов'язані з людським фактором:

- низька обізнаність працівників: брак навчання з питань кібербезпеки.

- порушення правил доступу: передача облікових даних стороннім особам.

6. Ризики через недостатність ресурсів:

- брак фінансування: недостатні інвестиції в оновлення систем безпеки.

- старе обладнання та ПЗ: використання застарілих технологій, які легко скомпрометувати.

В таблиці 1.4. представлена узагальнена характеристика ризиків

Таблиця 1.4.

Узагальнена характеристика ризиків

Категорія ризику	Джерело загрози	Можливі наслідки
Технічні	Збої обладнання, вразливості ПЗ	Втрата даних, зупинка бізнес-процесів
Організаційні	Відсутність політики безпеки	Неконтрольований доступ до інформації
Зовнішні	Хакерські атаки, соціальна інженерія	Крадіжка конфіденційних даних
Внутрішні	Дії працівників, людський фактор	Компрометація систем, фінансові збитки

Джерело: створено автором

Правильна ідентифікація та характеристика ризиків інформаційної безпеки дозволяє вчасно реагувати на загрози, знижуючи їх вплив на корпоративну інформаційну систему.

В таблиці 1.5. представлені способи управління ризиками інформаційної безпеки

Таблиця 1.5.

Способи управління ризиками інформаційної безпеки

Стратегія	Характеристика
Зменшення ризику	Впровадження технічних та організаційних заходів для мінімізації загроз.
Уникнення ризику	Усунення умов, що сприяють виникненню ризику.
Передача ризику	Використання страхування або залучення зовнішніх спеціалістів.
Прийняття ризику	Визнання ризику та підготовка до його ймовірних наслідків.

Джерело: створено автором

Управління ризиками в корпоративних системах може бути здійснене за допомогою різних стратегій, кожна з яких має свої особливості та сферу застосування.

1. **Зменшення ризику** є найбільш активною стратегією, орієнтуючись на впровадження заходів, які прямо впливають на зниження ймовірності або наслідків загрози. Ця стратегія є важливою для забезпечення безпеки в інформаційних системах.

2. **Уникнення ризику** ефективне, коли ризик має високу ймовірність або серйозні наслідки, і коли усунення умов, що його породжують, є практично можливим і доцільним.

3. **Передача ризику** стає корисною у випадках, коли організація не має можливості або не бажає самостійно брати на себе всю відповідальність, і може дозволити собі розподіляти частину ризиків на сторонні організації, наприклад, за допомогою страхування.

4. **Прийняття ризику** використовується у випадках, коли вартості запобігання ризику надто високі, або ж його наслідки є прийнятними для компанії. Це може бути виправдано в умовах, коли втрати від ризику прогнозуються як незначні або коли усунення ризику є непрактичним.

Таким чином, вибір стратегії управління ризиками залежить від специфіки кожного окремого випадку та ресурсів компанії для впровадження заходів по їх зменшенню чи перенесенню.

Висновок до розділу 1

Розробка та впровадження корпоративних інформаційних систем є важливим етапом у розвитку організацій, що прагнуть до оптимізації своїх бізнес-процесів і забезпечення ефективного управління. Теоретичні основи цієї діяльності включають вивчення різних підходів до проектування, інтеграції та використання інформаційних систем, які відповідають специфічним потребам організації та сприяють її розвитку.

1. Роль корпоративних інформаційних систем полягає в автоматизації та інтеграції ключових бізнес-процесів, що дозволяє підвищити продуктивність, зменшити витрати та поліпшити контроль за всіма аспектами діяльності. Використання таких систем забезпечує ефективне управління інформацією, що є основою прийняття обґрунтованих та своєчасних рішень.

2. Процес розробки корпоративної інформаційної системи є багатогранним і включає етапи від збору вимог до проектування, реалізації та тестування. Важливою частиною є вибір технологій, що дозволяють організації ефективно вирішувати свої завдання та мінімізувати ризики, пов’язані з інформаційною безпекою та інтеграцією з іншими системами.

3. Впровадження корпоративної інформаційної системи вимагає не лише технічного забезпечення, а й організаційних змін, оскільки нові системи часто потребують адаптації існуючих бізнес-процесів. Тому важливу роль відіграють навчання персоналу, підготовка змін в організаційній структурі та взаємодії між підрозділами.

4. Теоретичні підходи до розробки включають аналіз та вибір відповідних методологій, таких як водоспадна модель, моделі гнучкого управління проектами або методи моделювання процесів. Оцінка вимог і специфікацій для майбутньої системи є основою для успішної реалізації проекту.

5. Виклики, пов'язані з впровадженням, включають управління змінами, вибір правильних інструментів для забезпечення інтеграції, а також забезпечення високого рівня безпеки даних. Крім того, важливо враховувати потреби користувачів та забезпечити їхній комфорт при роботі з новою системою.

Загалом, теоретичні основи розробки та впровадження корпоративних інформаційних систем формують міцну базу для практичного застосування технологій у бізнесі, що дозволяє компаніям досягати високої ефективності, зменшувати ризики та забезпечувати стійкість у конкурентному середовищі.

РОЗДІЛ 2
ОЦІНКА РИЗИКІВ ПРИ ВПРОВАДЖЕННІ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Організаційна характеристика підприємства ПрАТ «Тернопільський молокозавод»

Предметом магістерського дослідження є аналіз розвитку ключових сфер діяльності підприємства з метою підвищення його конкурентоспроможності на ринку молочної продукції. Об’єктом дослідження обрано ПрАТ «Тернопільський молокозавод», заснований у 1956 році, який з моменту створення спеціалізується на виробництві та реалізації молока і молочних продуктів. Наразі підприємство є одним із найпотужніших і найуспішніших у західному регіоні України. Воно щоденно переробляє понад 400 тонн продукції, а чисельність персоналу сягає до 1500 осіб залежно від масштабу виробничої діяльності.

У 2011 році підприємство стало акціонерним товариством, а його продукція випускається під брендом ТМ «Молокія». Компанія займається виробничо-господарською діяльністю, впроваджує інноваційні технології та стала першою в Україні, яка використовує технологію «Свіже молоко». Уся продукція підприємства сертифікована за стандартом якості ISO 22000:2005, що підтверджує її високу якість і конкурентоспроможність [16].

На підприємстві сформовано ефективну та раціональну організаційну структуру, яка повністю відповідає його специфіці. Ця структура побудована за функціонально-лінійним принципом і показана на рис.2.1

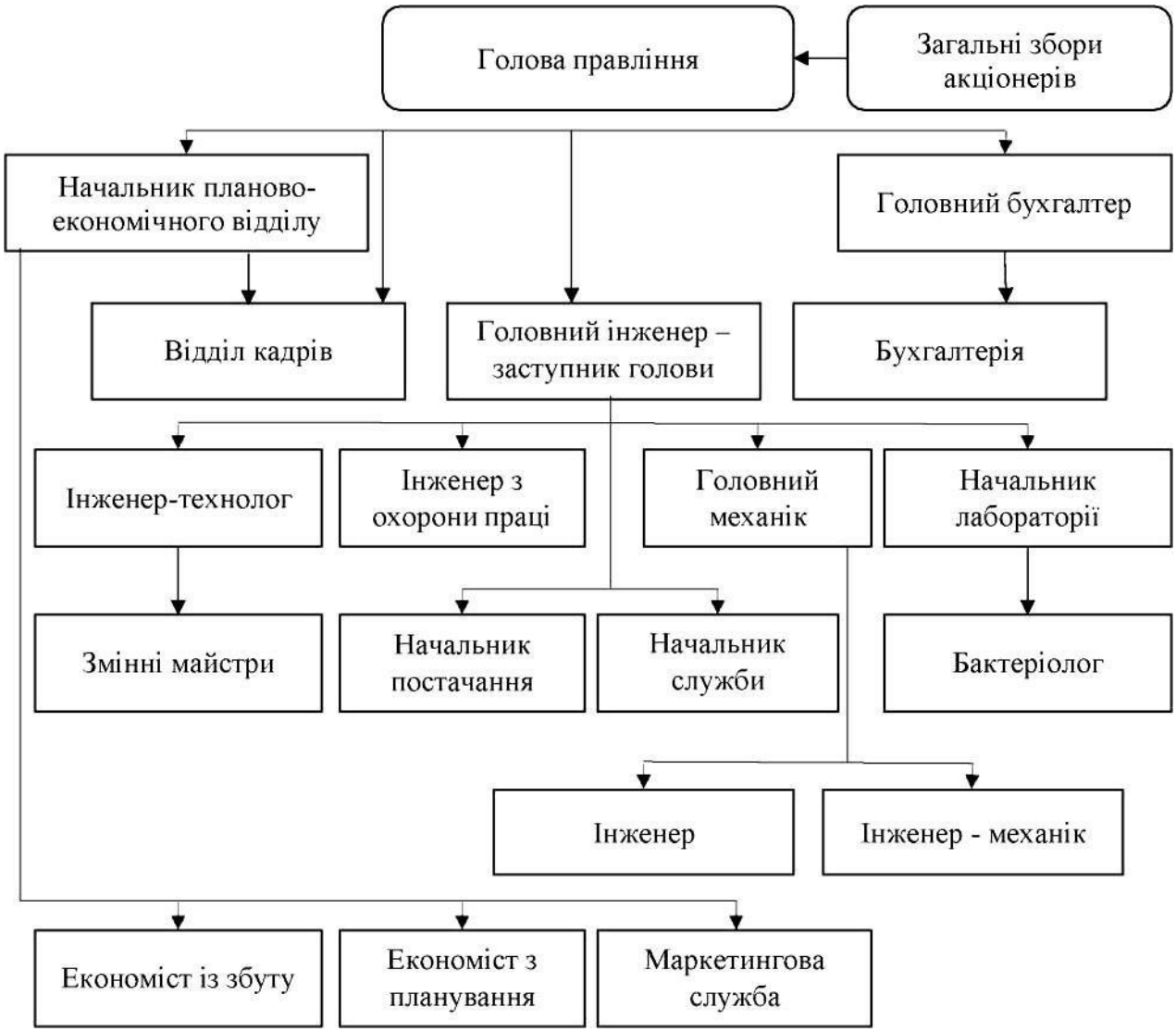

Рисунок 2.1. Організаційна структура ПрАТ «Тернопільський молокозавод ».

Аналізуючи існуючу організаційну структуру підприємства, слід відзначити наявність ключових підрозділів, таких як відділ кадрів, планово-економічний відділ, бухгалтерія, відділ охорони праці, інженерний відділ та відділ маркетингу. Управління підприємством здійснюється директором, який володіє широкими повноваженнями в організації та забезпеченні роботи компанії. Він визначає фінансову, кадрову, інноваційну та інші напрями діяльності підприємства. Для оцінки ефективності роботи компанії на ринку буде проведено аналіз

фінансово-економічних показників ПрАТ «Тернопільський маслозавод» за 2020–2023 роки та наведено дані в таблиці 2.1.

Таблиця 2.1

Фінансово-економічні показники діяльність компанії ПрАТ «Тернопільський маслозавод» на 2019-2023 роки, тис.грн

Показники	**Роки**				
	2019	2020	2021	2022	2023
I. Показники звіту про фінансовий стан підприємства					
Активи (Пасиви)	832083	856423	958019	1033242	1273995
Основні засоби	489890	495926	497760	477776	439242
Дебіторська заборгованість	187077	169359	147513	185336	261796
Запаси	85590	90109	131526	133058	222198
Власний капітал	434722	400919	449291	424500	625146
Довгострокові зобов’язання	176799	193724	104670	36622	149218
Поточні зобов'язання	220562	261780	404265	572120	499631
Довгострокові кредити банків	123138	147296	59873	118681	229937
Короткострокові кредити банків	17256	17125	14915	18581	-
II. Показники звіту про фінансові результати					
Чистий дохід від реалізації продукції	1799343	1752721	2326475	3497941	4038979
Собівартість реалізації	1382956	1505362	2092681	1689249	3476149
Валовий прибуток	416387	247359	233794	302138	562830
Адміністративні витрати	35888	44162	47558	40711	98487
Витрати на збут	276595	161446	138585	130184	222701
Прибуток до оподаткування	52678	58064	56875	242948	145085
Чистий прибуток	42905	-33803	-31567	-31783	11164
III. Показники ефективності праці на підприємстві					
Кількість працівників	1432	1494	1494	1365	1478
Фонд оплати праці	143087	205803	210890	207645	245760
Продуктивність праці	1256,52	1173,17	1175,45	1075,54	1175,45

Аналіз показників, представлених у таблиці 2.1, свідчить про позитивну динаміку діяльності ПрАТ «Тернопільський молокозавод», незважаючи на складну політичну ситуацію та військові дії на території України з лютого 2022 року. Хоча 2022 рік став складним періодом через війну, зменшення фінансових показників торкнулося лише деяких позицій:

- Основні засоби зменшилися з 497 760 тис. грн у 2021 році до 477 776 тис. грн, що становить зниження на 19 984 тис. грн. Це могло бути зумовлено частковою втратою обладнання або зниженням інвестицій у розвиток.

- Власний капітал також скоротився з 449 291 тис. грн до 424 500 тис. грн (на 24 791 тис. грн). Це свідчить про тимчасове скорочення фінансових ресурсів підприємства.

- Кількість працівників зменшилася, що можна пояснити виїздом людей за кордон, внутрішньою міграцією та втратою робочих місць унаслідок обстрілів та економічної кризи.

Разом із цим, деякі показники демонстрували позитивну динаміку:

- Чистий прибуток та валовий дохід зросли, що вказує на стійкість попиту на продукцію підприємства навіть в умовах кризи.

У 2023 році ПрАТ «Тернопільський молокозавод» зумів не лише відновити, але й покращити свої фінансово-економічні показники:

- Чистий дохід зріс до 4 038 979 тис. грн, що на 541 038 тис. грн більше, ніж у 2022 році. Це свідчить про активне відновлення ринків збуту та збільшення обсягів реалізації.

- Валовий і чистий прибуток також зросли, підтверджуючи ефективність управлінських рішень і адаптацію до умов ринку.

Збільшення основного капіталу підприємства свідчить про проведення модернізації виробничих потужностей, впровадження передових технологій і новітнього обладнання. Підприємство орієнтоване на розвиток інновацій, незважаючи на складні зовнішні обставини. Зокрема, ПрАТ «Тернопільський молокозавод» стало першою компанією в Україні, яка застосувала німецьку «технологію свіжого молока». Це забезпечує високу якість продукції, що сприяє утриманню конкурентних позицій на ринку та знижує ризик корпоративної інформаційної безпеки.

Підприємство демонструє високу адаптивність до зовнішніх викликів, таких як війна та економічна нестабільність. Позитивна динаміка фінансових показників у 2023 році свідчить про успішне подолання кризи 2022 року. Інвестиції в інновації та модернізацію основних засобів забезпечують зростання конкурентоспроможності та стабільний розвиток у довгостроковій перспективі. ПрАТ «Тернопільський молокозавод» є прикладом стійкого підприємства, яке в умовах війни не тільки зберегло, а й розвиває свою діяльність, спрямовуючи зусилля на покращення якості продукції та впровадження інновацій.

Аналізуючи дебіторську заборгованість підприємства, слід зазначити її зростання на 76 460 тис. грн у 2023 році, що негативно впливає на структуру капіталу та потребує вирішення проблем, пов'язаних із накопиченням такої заборгованості. Збільшення масштабів виробничо-господарської діяльності стимулює підприємство до накопичення власних запасів. Динаміка змін активів компанії представлена на рис. 2.2.

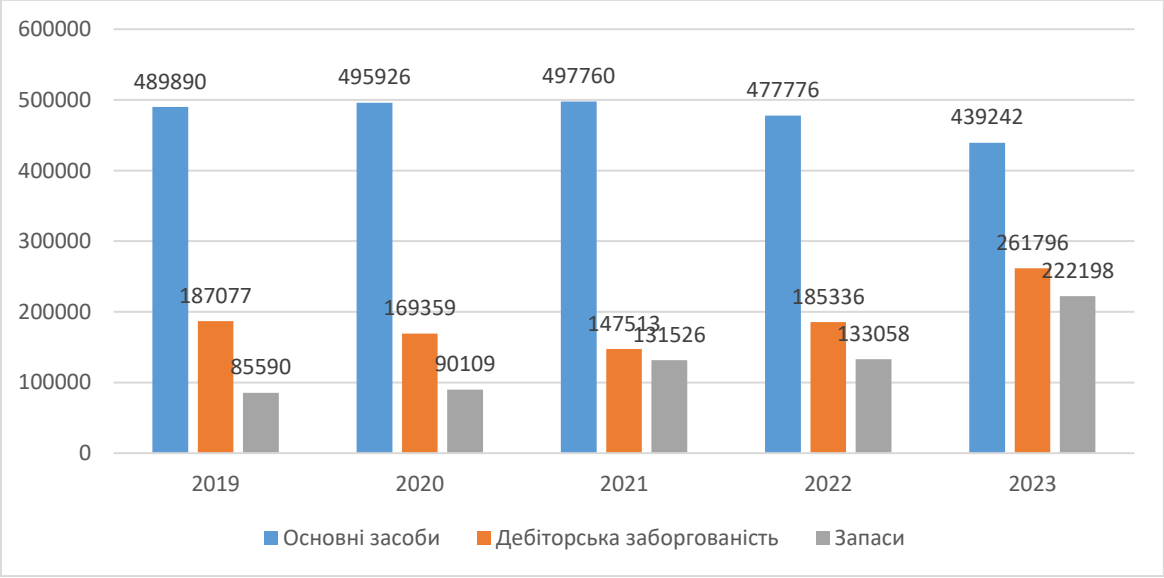

Рисунок 2.2. Динаміка розвитку активів компанії 2019-2023 роки [створено автором]

Згідно з даними, дебіторська заборгованість ПрАТ «Тернопільський молокозавод» зросла зі 147 513 тис. грн у 2021 році до 185 336 тис. грн у 2022 році, а в 2023 році досягла 261 796 тис. грн. Приріст у 2023 році порівняно з 2022 роком становить 141%. Таке суттєве зростання вимагає вдосконалення механізмів управління дебіторською заборгованістю для збереження фінансової стійкості підприємства.

Структура пасивів, що враховує частку власного капіталу та зобов'язань (короткострокових і довгострокових), має важливе значення для забезпечення корпоративної інформаційної безпеки та управління ризиками. Наявність стабільного власного капіталу, зокрема додаткового капіталу й нерозподіленого прибутку, який зростає навіть за умов воєнних дій, свідчить про фінансову стійкість підприємства. Це дозволяє спрямовувати ресурси на захист інформаційних систем, впровадження сучасних технологій для моніторингу та запобігання кібератакам, а також розробку стратегій реагування на ризики.

У періоди нестабільності, такі як війна, підприємства стають більш вразливими до інформаційних загроз, включаючи шахрайство, витік даних або порушення роботи критичних систем. Надійна структура пасивів дозволяє інвестувати в розбудову інформаційної безпеки, впровадження систем резервного копіювання та управління ризиками, що мінімізує можливі втрати та підтримує стійкість бізнесу.

Таким чином, фінансова стабільність через ефективне управління пасивами є важливим фактором зниження корпоративних ризиків, пов'язаних з інформаційною безпекою.

Упродовж усього аналізованого періоду підприємство використовувало короткострокові банківські кредити, які спрямовувалися на оновлення основного капіталу, реалізацію маркетингових заходів для просування нових продуктів та організацію навчання персоналу.

Динаміку зобов'язань та пасивів ПрАТ «Тернопільський молокозавод» за 2019-2023 роки наведено на рисунку 2.3.

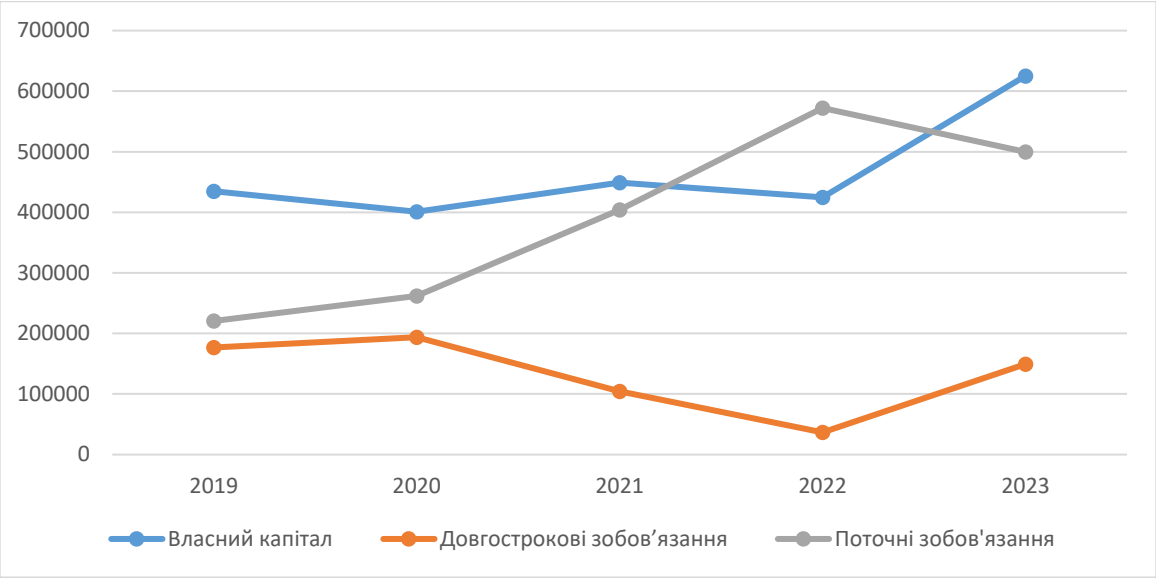

Рисунок 2.3. Динаміка зоов’язань та пасивів ПрАТ «Тернопільський молокозавод» за період 2019-2023 р.р. [створено автором]

Діяльність компанії значною мірою базується на позиковому капіталі, причому в структурі джерел фінансування активів переважають короткострокові зобов’язання, які відіграють домінуючу роль у фінансуванні активів.

Наступним етапом є аналіз основних фінансових результатів підприємства. У цьому контексті слід зазначити, що протягом досліджуваного періоду відбулося збільшення чистого доходу від реалізації. Окрім цього, зросла собівартість реалізованої продукції, яка підвищилася з 1 382 956 тис. грн у 2019 році до 3 476 149 тис. грн у 2023 році. Приріст цього показника становить 2 093 193 тис. грн, або 251% за весь період аналізу.

Також протягом звітного періоду спостерігалося зростання адміністративних та збутових витрат, темпи зростання яких склали 67,65% та 87,97% відповідно.

Динаміка чистого прибутку даного підприємства представлена на рис. 2.4.

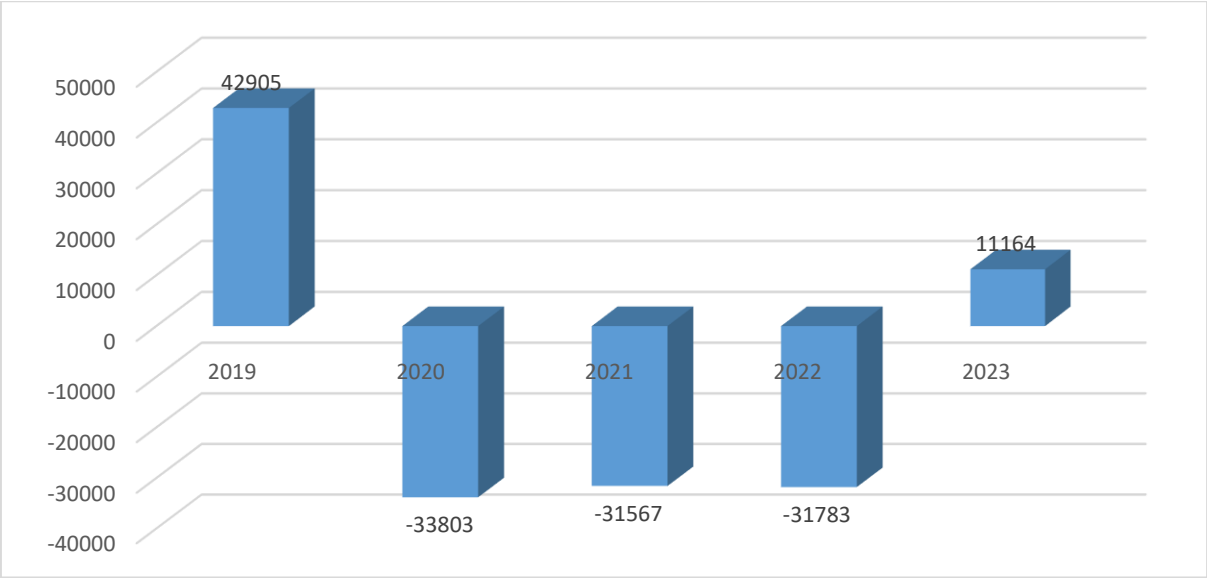

Рисунок 2.4. Динаміка змін чистого прибутку (збитку) ПрАТ «Тернопільський молокозавод» за 2019-2023 роки [створено автором].

Згідно з даними рисунку 2.4, підприємство зазнало збитків, що обумовлено збільшенням витрат і зниженням темпів приросту активності. ПрАТ «Тернопільський молокозавод» зіткнулося зі зниженням рентабельності своєї виробничо-господарської діяльності, а потім війна ще більше погіршила ситуацію, що призвело до збитковості підприємства за звітний період. Показник чистого прибутку знижувався протягом 2019–2022 років, і лише у 2023 році вдалося досягти позитивного результату. Це стало можливим завдяки впровадженню інноваційних технологій та змінам у політиці підприємства.

Підсумовуючи основні показники діяльності підприємства (активи та пасиви, власний капітал, основні фонди, чисельність працівників, продуктивність праці), слід зазначити, що витрати на реалізацію продукції зросли, посилилася залежність від позикового капіталу, а також вплинула війна в країні. Починаючи з 2020 року, компанія зафіксувала збитки, які тривали ще два роки. Однак, при визначенні стратегічних рішень для виведення підприємства з кризи та його стабілізації, важливо звернути увагу на позитивні аспекти діяльності, які були зафіксовані протягом

досліджуваного періоду. З іншого боку, основною проблемою неефективності діяльності є зниження конкурентоспроможності підприємства як на внутрішньому, так і на зовнішньому ринках, що пов'язано з нестабільною політичною та економічною ситуацією, а також війною в країні. Ці фактори створюють додаткові ризики для бізнесу, зокрема у сфері корпоративної інформаційної безпеки. У кризових умовах, коли відбувається зміна структури капіталу та збільшуються фінансові зобов'язання, важливо мати належний рівень інформаційної безпеки для захисту від кіберзагроз та збереження конфіденційності даних.

Управління ризиками, включаючи інформаційні загрози, має стати пріоритетом для підприємства, оскільки ефективна система інформаційної безпеки допомагає не лише запобігати витокам даних та іншим загрозам, а й знижувати загальний рівень фінансових та операційних ризиків у період нестабільності. Це дозволить підприємству залишатись конкурентоспроможним та адаптованим до змінюваного ринкового середовища.

2.2. Аналіз фінансової та виробничої сфер підприємства в умовах корпоративної інформаційної безпеки

Аналіз фінансової та виробничої сфер підприємства в умовах корпоративної інформаційної безпеки є важливим аспектом управління бізнесом, оскільки в умовах сучасної економіки та технологічних змін захист інформації та ефективне використання фінансових і виробничих ресурсів нерозривно пов'язані. Основні етапи аналізу включають наступне:

1. Аналіз фінансової сфери підприємства в умовах корпоративної інформаційної безпеки. Фінансова сфера підприємства включає управління доходами, витратами, прибутком, а також залученням позикових коштів і власного капіталу. У сучасних умовах, коли підприємства стикаються з

кібератаками, шахрайством і витоками інформації, важливість корпоративної інформаційної безпеки для фінансової сфери неможливо переоцінити.

- Управління фінансовими даними. Для запобігання несанкціонованому доступу до фінансової інформації та захисту від фінансових шахрайств важливо впроваджувати системи шифрування даних і доступу, багаторівневу аутентифікацію і системи моніторингу фінансових транзакцій.
- Аналіз фінансових ризиків. Інформаційна безпека дозволяє забезпечити цілісність і конфіденційність фінансової звітності. Недосконала система безпеки може призвести до маніпуляцій з фінансовими звітами, що в свою чергу підвищує ризики неефективного управління фінансами.
- Взаємодія з партнерами та постачальниками. Захист даних про фінансові операції і умови контрактів з партнерами є критично важливим для збереження конкурентоспроможності та уникнення витоків стратегічної інформації.

2. Аналіз виробничої сфери підприємства в умовах корпоративної інформаційної безпеки. Виробнича сфера підприємства включає управління виробничими процесами, ресурсами та технологіями, що забезпечують виробництво продукції або надання послуг. В умовах інтенсивної цифровізації та автоматизації виробництво все більше залежить від інформаційних систем і технологій.

- Захист виробничих даних. Всі процеси, від планування виробництва до управління запасами, мають цифрове відображення. Зловмисники, які отримують доступ до виробничих систем, можуть зупинити виробництво, викрасти важливі дані або навіть змінити параметри технологічного процесу, що може призвести до зниження якості продукції або збитків.

- Інтеграція інформаційних систем. Впровадження систем управління підприємством (ERP-систем), автоматизація процесів і використання інтернету речей (IoT) підвищують ефективність, але також створюють нові ризики для безпеки. Інформаційні системи, які обробляють дані про запаси,

виробничі потужності та логістичні операції, повинні бути захищені від атак, щоб уникнути порушень у постачанні і виробництві.

- Управління ризиками в виробничих процесах. Важливо не тільки контролювати виробничі витрати та продуктивність праці, а й бути готовими до оперативного реагування на загрози, пов’язані з кібербезпекою. Система управління ризиками повинна включати плани реагування на інциденти інформаційної безпеки та заходи для відновлення роботи у разі атак на виробничі процеси.

3. Зв'язок фінансової та виробничої сфер через інформаційну безпеку

- Оптимізація ресурсів та мінімізація витрат. Наявність систем інформаційної безпеки забезпечує надійність фінансових і виробничих процесів, дозволяючи ефективно керувати ресурсами та мінімізувати витрати на відновлення після інцидентів. Це дозволяє підприємству підтримувати стійкість в умовах невизначеності.

- Забезпечення безпеки ланцюга постачань. Взаємодія між фінансовою та виробничою сферами вимагає постійного моніторингу інформаційних потоків, щоб уникнути зривів у ланцюгах постачання або втрат при фінансуванні. Система безпеки повинна захищати не лише внутрішні процеси, але й інформацію, що обмінюється з постачальниками та партнерами.

Інтеграція інформаційної безпеки у фінансові та виробничі процеси є ключовим фактором для забезпечення безперебійної роботи підприємства. Як для фінансової, так і для виробничої сфер, необхідно впроваджувати комплексні системи захисту, які мінімізують ризики, пов'язані з кіберзагрозами. Підвищення рівня корпоративної інформаційної безпеки дозволяє підприємству стабільно функціонувати навіть у нестабільних економічних і політичних умовах, зберігаючи високий рівень конкурентоспроможності на ринку. Ризики в обох сферах повинні враховуватись як взаємопов'язані, і будь-які порушення в інформаційній безпеці можуть мати серйозні наслідки для фінансової стабільності і виробничої ефективності підприємства. Наступним кроком для аналізу

розвитку структури ключових сфер підприємства в контексті управління його конкурентоспроможністю буде вивчення конкурентної позиції нашого об’єкта дослідження та його потенціал в умови діяльності на місцевому ринку молочних продуктів. Для початку визначимо основних конкурентів нашої компанії на ринку.

Проаналізуємо фінансові показники ПрАТ «Тернопільський молокозавод». Аналітичні дані представлені в таблиці 2.2.

Таблиця 2.2

Аналітичні дані ПрАТ «Тернопільський молокозавод» за період 2019-2023 рр., тис. грн.

Показники	Роки					Відхилення		
	2019	2020	2021	2022	2023	2021/ 2020	2022 2021	2023 2019
Вхідні дані								
Валові витрати	120219	170369	219253	349379	243996	48884	130126	123777
Обсяг випуску	997864	1348197	1751302	2069244	2015629	403104,9	317942,8	1017765
Вартість основних засобів	115642	152022	223515	489890	495926	71493	266375	380284
Дохід від реалізації	867708	1172345	1522871	1799343	1752721	350526	276472	885013
Собівартість	707475	970317	1228697	1382956	1505362	258380	154259	797887
Чисельність персоналу	1342	1286	1374	1432	1494	88	58	152
Розрахункові показники								
1. Відносний показник продукції (В)	0,12	0,13	0,13	0,17	0,12	- 0,001	0,044	0,001
2. Показник фондовіддачі (Ф)	8.63	8,87	7,84	4.22	4.06	- 1.03	- 3,61	- 4,56
3. Показник рентабельності товару (РТ)	1.23	1.21	1.24	1:30	1.16	0,03	0,06	- 0,06
4. Показник продуктивності праці (ПП)	743,56	1048,36	1274,60	1445,00	1349,15	226,24	170,40	605,58

Аналіз даних показує, що до 2022 року підприємство демонструвало позитивну динаміку в ключових показниках. Спостерігалося стабільне зростання обсягу випуску продукції, доходу від реалізації та вартості основних засобів, що свідчить про розвиток виробничих потужностей і розширення

діяльності. Продуктивність праці також поступово зростала, що є ознакою ефективного використання людських ресурсів.

Однак у 2023 році відзначається спад у багатьох аспектах діяльності. Зокрема, знизився обсяг випуску продукції, дохід від реалізації та рентабельність, тоді як собівартість і валові витрати залишалися на високому рівні. Падіння фондовіддачі та зниження продуктивності праці свідчать про менш ефективне використання ресурсів. Хоча чисельність персоналу збільшилася, це не сприяло поліпшенню загальної ефективності.

Ці зміни вказують на можливі внутрішні або зовнішні фактори, які вплинули на результати діяльності підприємства у 2023 році. Подальший розвиток потребує детального аналізу причин цих змін, перегляду витрат і пошуку шляхів для підвищення ефективності використання основних засобів та ресурсів.

В таблиці 2.3 надана динаміка ключових показників фінансового стану підприємства.

Таблиця 2.3.

Динаміка ключових показників фінансового стану ПрАТ «Тернопільський молокозавод» 2019-2023 роки.

Показники	Роки					Відхилення		
	2019	2020	2021	2022	2023	2021/ 2020	2022 2021	2023 2019
Вхідні дані								
Власний капітал	124965	138137	182779	434722	400919	44642	251943	275954
Загальна сума активів	266214	366174	468308	832083	856423	102134	363775	590209
Загальні зобов'язання	141249	228037	285529	397361	455504	57492	111832	314255
Грошові кошти	1830	3856	17316	6669	9109	13460	-10647	7279
Поточні зобов'язання	71593	105884	121578	220562	261780	15694	98984	190187
Дохід від реалізації	867708	1172345	1522871	1799343	1752721	350526	276472	885013
Обіговий капітал	132884	132480	210064	281133	269809	77584	71069	136925
Розрахункові показники								
1. Коефіцієнт автономії (КА)	0,47	0,38	0,39	0,52	0,47	0,01	0,13	0,00
2. Коефіцієнт покриття (поточної ліквідності) (КП)	1,88	1,61	1,64	2,09	1,88	0,03	0,45	0,00
3. Коефіцієнт абсолютної ліквідності (КЛ)	0,03	0,04	0,14	0,03	0,03	0,11	-0,11	0,01
4. Коефіцієнт оборотності обігових коштів (КО)	6,53	8,85	7,25	6,40	6,50	-1,60	-0,85	-0,03

Згідно з даними таблиці 2.3, варто звернути увагу на динамічне зростання корпоративної автономії підприємства, яке збільшилося з 0,38 бала у 2020 році до 0,52 бала у 2023 році. Це свідчить про підвищення рівня незалежності підприємства у фінансово-економічних рішеннях та зміцнення його фінансової стабільності.

Однак паралельно спостерігається акцент управління на використання позикового капіталу, що може свідчити про зростання зовнішніх фінансових зобов'язань. Така стратегія, з одного боку, може забезпечити додаткові ресурси для розвитку, але, з іншого боку, може збільшити фінансові ризики у разі несприятливих змін на ринку.

Також варто зазначити негативну тенденцію у зниженні швидкості оборотності оборотних коштів. Це може вказувати на недостатню ефективність управління ресурсами або складнощі із реалізацією продукції, що уповільнює обіговість капіталу. У перспективі такі зміни можуть створювати додатковий тиск на фінансову стабільність підприємства, знижуючи його ліквідність та впливаючи на можливість своєчасного виконання зобов'язань.

У цілому, спостережувані зміни вимагають подальшого аналізу та коригування управлінських стратегій для забезпечення збалансованого використання ресурсів, підтримання високого рівня корпоративної автономії та прискорення обігу оборотних коштів.

Таким чином, ПрАТ «Тернопільський молокозавод» демонструє потенціал до конкурентної боротьби на ринку завдяки стабільності у фінансовій та виробничій сферах, що є важливим елементом корпоративної безпеки. Фінансовий аналіз засвідчує стабільність підприємства, яка відображається у його прибутковості, ліквідності та платоспроможності. Ці характеристики сприяють підвищенню фінансової стійкості, що мінімізує ризики втрати економічної незалежності і забезпечує довгострокову стабільність. У виробничій сфері ефективність процесів, раціональне використання ресурсів та конкурентоспроможність виробничих пропозицій підтверджують здатність підприємства адаптуватися до змін ринкових умов. Це не лише зміцнює позиції на ринку, а й посилює стійкість до зовнішніх загроз, таких як зростання конкуренції чи економічні кризи.

Отже, здатність підтримувати високі показники у фінансовій та виробничій сферах сприяє загальному зміцненню корпоративної безпеки ПрАТ «Тернопільський молокозавод». Це забезпечує підприємству можливість залишатися стабільним та конкурентоспроможним навіть у складних ринкових умовах.

Підсумовуючи, слід підкреслити ключові переваги підприємства, такі як стабільна фінансова основа та ефективна організація виробничих процесів, що

забезпечують його конкурентоспроможність і сприяють зміцненню корпоративної безпеки. Водночас важливо врахувати потенційні ризики, зокрема нестабільність ринкової ситуації або нераціональне використання ресурсів, які можуть вплинути на стійкість підприємства та його здатність адаптуватися до змін.

Аналіз конкурентоспроможності дозволяє підприємству не лише оцінити своє поточне становище на ринку, а й виявити потенційні загрози для його фінансової та операційної безпеки. Це сприяє розробці стратегій, спрямованих на мінімізацію ризиків, підвищення ефективності використання ресурсів та адаптацію до зовнішніх викликів, що є основою для довгострокового успішного функціонування та розвитку.

Загальний розвиток конкурентоспроможного потенціалу досліджуваної компанії демонструє позитивну динаміку, оскільки зростання цього показника за період з 2019 до 2023 року склало 1,91 рази. Це свідчить про ефективність управління та стійкість до зовнішніх викликів, що є важливими елементами забезпечення корпоративної безпеки.

Однак у 2023 році, під впливом військового стану та нестабільності політичної й економічної ситуації в країні, спостерігалося незначне зниження конкурентоспроможності компанії. Незважаючи на це, масштаби падіння були мінімальними, що свідчить про здатність підприємства адаптуватися до екстремальних умов та підтримувати стабільність своїх операцій.

Ця стійкість є важливим фактором забезпечення економічної та стратегічної безпеки компанії, дозволяючи їй зберігати свої позиції на ринку навіть у кризових умовах. Надалі підприємству слід зосередитися на подальшому зміцненні своїх конкурентних переваг та управлінні ризиками для забезпечення стабільного розвитку та безпеки.

2.3. Оцінка ризиків при впровадженні корпоративної інформаційної безпеки на ПрАТ «Тернопільський молокозавод»

Результати аналітичної оцінки вказують на суттєвий вплив ризикових факторів на діяльність досліджуваного підприємства. При цьому система ризик-менеджменту наразі представлена лише окремими фрагментами, що підкреслює важливість розробки й впровадження цілісного та ефективного механізму управління ризиками для мінімізації негативних впливів та підвищення стійкості підприємства.

Питання створення спеціального підрозділу з управління ризиками та можливість утримання у штаті професійних ризик-менеджерів є предметом дослідження як вітчизняних, так і зарубіжних науковців. Результати цих досліджень свідчать про доцільність формування на великих підприємствах окремих структурних підрозділів або призначення відповідальних осіб за управління різними видами ризиків. Водночас відзначається обмеженість ринку кваліфікованих фахівців із досвідом у сфері ризик-менеджменту, що створює додаткові виклики для підприємств у впровадженні ефективної системи управління ризиками.

Ризик-менеджер має володіти знаннями про технологію виробництва та управлінські процеси, добре розуміти продукцію підприємства, а також внутрішні та зовнішні чинники, що можуть впливати на його діяльність. Крім того, він повинен мати досвід роботи, розвинути математичні та аналітичні навички, бути стійким до стресів і здатним ухвалювати рішення при обмеженій інформації.

Обмежуючим фактором, який впливає на прийняття ризикового рішення, є психологічна готовність управлінця до ризику. На його здатність ухвалювати ризиковані рішення впливають психологічні характеристики особистості, зокрема, її схильність до адаптації до зовнішнього (екстравертність) і внутрішнього (інтравертність) середовища. Екстравертність проявляється у прагненні впливати на зовнішнє середовище

через маневрування ресурсами, маніпулювання поведінкою партнерів, кредиторів і споживачів під час укладання угод. Інтравертність, у свою чергу, характерна для осіб, які не вірять у постійний контроль над зовнішнім середовищем і вважають за краще збирати додаткову інформацію, генерувати альтернативні ідеї, вигравати час і залучати керівництво до прийняття важливих рішень. Маючи ці риси, менеджер з управління ризиками здатний прогнозувати та моделювати різноманітні ризикові ситуації.

Основними завданнями ризик-менеджера є:

– виявлення та формулювання проблем, що регулярно виникають;

– збір, організація та аналіз інформації про ризики;

– постійний моніторинг рівня ризику, який виникає під час діяльності підприємства;

– управління рівнем ризику, що пов'язаний з процесом прийняття рішень.

Визначаючи особливості формування системи управління ризиками на ПрАТ «Тернопільський молокозавод», слід наголосити що важливою складовою є інтеграція корпоративної інформаційної безпеки в процес управління підприємством. Формування системи управління ризиками на ПрАТ «Тернопільський молокозавод» вимагає врахування багатьох факторів, серед яких інтеграція корпоративної інформаційної безпеки (КІБ) є надзвичайно важливою складовою. Інформаційна безпека є критичною для захисту даних підприємства, безперервності його діяльності, а також для збереження корпоративної репутації та конкурентоспроможності на ринку.

В таблиці 2.4, наведено деякі з аспектів інтеграції корпоративної інформаційної безпеки в систему управління ризиками на досліджуємому підприємстві.

Таблиця 2.4

Аспекти інтеграції корпоративної інформаційної безпеки в систему управління ризиками на ПрАТ «Тернопільський молокозавод»

Аспект інтеграції КІБ	Характеристика
1. Оцінка інформаційних ризиків	Аналіз потенційних загроз і вразливостей інформаційних систем, що можуть вплинути на діяльність підприємства.
2. Розробка політики безпеки	Створення чітких регламентів та процедур для захисту інформації від несанкціонованого доступу, зміни чи втрати.
3.Впровадження технічних засобів захисту	Використання сучасних програмних і апаратних засобів для забезпечення безпеки корпоративних даних (антивірусне ПЗ, фаєрволи, IDS).
4. Навчання персоналу	Підготовка працівників до роботи в умовах інформаційної безпеки та формування культури обережності при роботі з даними підприємства.
5. Моніторинг і реагування на інциденти	Постійний контроль за станом безпеки інформаційних систем і швидке реагування на можливі порушення або атаки.

Інтеграція корпоративної інформаційної безпеки (КІБ) в систему управління ризиками на підприємстві є важливим і багатоступінчатим процесом, який охоплює різні аспекти захисту інформації. Всі етапи цієї інтеграції — від оцінки інформаційних ризиків до моніторингу та реагування на інциденти — сприяють створенню надійної системи безпеки, що забезпечує захист від загроз і вразливостей.

1. Оцінка ризиків дає змогу ідентифікувати потенційні загрози, що можуть зашкодити підприємству, в той час як розробка політики безпеки визначає чіткі правила і процедури для захисту інформації.

2. Впровадження технічних засобів захисту гарантує використання сучасних технологій для захисту даних від зовнішніх і внутрішніх загроз.

3. Навчання персоналу забезпечує підвищення рівня обізнаності працівників, що допомагає знизити людський фактор у виникненні інцидентів безпеки.

4. Моніторинг та реагування на інциденти дозволяють своєчасно виявляти та ліквідовувати загрози, мінімізуючи їх негативний вплив на діяльність підприємства.

Завдяки такій комплексній інтеграції, система управління ризиками стає більш стійкою до інформаційних атак і інших загроз, що позитивно впливає на стабільність і безперервність роботи підприємства.

Для ефективного управління корпоративною інформаційною безпекою на підприємстві важливо визначити основні показники, що дозволяють оцінити рівень захищеності інформаційних ресурсів. В таблиці 2.5 представлено інтеграцію корпоративної інформаційної безпеки (КІБ) в систему управління ризиками на ПрАТ «Тернопільський молокозавод», з врахуванням основних аспектів і показників КІБ:

Таблиця 2.5.

Основні показники корпоративної інформаційної безпеки в системі управління ризиками на ПрАТ «Тернопільський молокозавод»

Аспект інтеграції КІБ	Характеристика для ПрАТ «Тернопільський молокозавод»	Основні показники КІБ	Характеристика
Оцінка інформаційних ризиків	Аналіз потенційних загроз для інформаційних систем заводу, зокрема, можливих кіберзагроз, атак на бази даних, збоїв в автоматизованих системах управління виробництвом.	Рівень захищеності даних	Кількість випадків несанкціонованого доступу або порушення конфіденційності даних підприємства.
Розробка політики безпеки	Створення внутрішніх регламентів, правил доступу до інформаційних систем, а також процедур на випадок витоку даних чи порушення	Час відновлення після інцидентів	Час, необхідний для відновлення роботи підприємства після інформаційної атаки чи технічних збоїв.

	інформаційної безпеки.		
Впровадження технічних засобів захисту	Використання антивірусних програм, фаєрволів, систем виявлення вторгнень для захисту корпоративних даних та автоматизованих систем виробництва.	Кількість навчальних програм	Кількість співробітників, що пройшли тренінги або сертифікацію з інформаційної безпеки для роботи з корпоративними даними.
Навчання персоналу	Підготовка працівників до роботи з інформаційними системами та формування у них культури обережності для запобігання витоку або несанкціонованому доступу до даних підприємства.	Частота виявлення вразливостей	Кількість нових вразливостей в системах безпеки, виявлених у процесі аудиту або тестування захищеності інформаційних ресурсів.
Моніторинг і реагування на інциденти	Постійний контроль за безпекою інформаційних систем, своєчасне реагування на потенційні інциденти, включаючи спроби злому, виявлення аномальних дій у системах.	Індикатор ефективності інцидентів безпеки	Кількість успішно знешкоджених інцидентів безпеки в порівнянні з тими, що мали серйозні наслідки для підприємства.
		Процент успішних захистів від загроз	Частка спроб кібернападів, які були успішно відхилені завдяки технічним засобам захисту, таких як фаєрволи та антивіруси.
		Індикатор рівня комплаєнсу	Відповідність корпоративних процесів і політик інформаційної безпеки стандартам, таким як ISO/IEC 27001, GDPR,

			зокрема для захисту персональних даних.

Інтеграція корпоративної інформаційної безпеки (КІБ) в систему управління ризиками на ПрАТ «Тернопільський молокозавод» є невід'ємною частиною забезпечення стабільності та безпеки підприємства. Важливими аспектами є не лише технічні засоби захисту, але й активне навчання персоналу, чітка політика безпеки та постійний моніторинг і реагування на інциденти. Визначення та аналіз показників КІБ дозволяє оцінити ефективність цих заходів і забезпечити захист корпоративних даних від зовнішніх і внутрішніх загроз.

На рисунку 2.5. представлена схема, яка описує процес інтеграції корпоративної інформаційної безпеки в систему управління ризиками на ПрАТ «Тернопільський молокозавод».

Рисунок 2.5. - Процес інтеграції корпоративної інформаційної безпеки в систему управління ризиками на ПрАТ «Тернопільський молокозавод»

При визначенні інформаційних ризиків проводиться оцінка й аналіз загроз для інформаційних ресурсів підприємства. При оцінці потенційних загроз та вразливостей відбувається визначення можливих уразливих точок і факторів ризику. Розробка політики безпеки дозволяє формулювати стратегії та процедури, що гарантують захист даних. При впровадженні технічних засобів захисту відбувається встановлення програмних і апаратних засобів для захисту корпоративної інформації. Навчання персоналу стимулює створення програми навчання для підвищення обізнаності щодо інформаційної безпеки. Моніторинг і реагування на інциденти – це постійний контроль стану безпеки і швидке реагування на інциденти. На етапі оцінки ефективності захисту відбувається вимірювання результатів через показники ефективності та аналіз ступеня захищеності даних.

Ця схема дозволяє створити комплексну систему управління ризиками, що враховує важливість інформаційної безпеки для забезпечення стабільної діяльності підприємства.

Оцінка ризиків в корпоративній інформаційній безпеці для ПрАТ «Тернопільський молокозавод» є важливим етапом у створенні стійкої системи захисту даних і інформаційних ресурсів підприємства. Окрім основних аспектів, можна додати такі елементи до оцінки ризиків:

1. Ідентифікація критичних інформаційних активів - ідентифікація найбільш важливих для підприємства інформаційних ресурсів, таких як бази даних клієнтів, фінансова інформація, технологічні процеси, інтелектуальна власність (наприклад, рецептури молокопродуктів), а також критичні програмні засоби.

2. Аналіз потенційних внутрішніх загроз - оцінка ризиків, що виникають через недобросовісних співробітників, внутрішні помилки або недогляди. Це може включати ризики, пов'язані з несанкціонованим доступом до важливих даних або витоком конфіденційної інформації через недбалість персоналу.

3. Оцінка загроз з боку партнерів і постачальників - оцінка ризиків, пов'язаних з партнерськими відносинами або зовнішніми постачальниками послуг, що мають доступ до інформаційних систем або даних підприємства. Це включає ризики витоку даних або вразливості, пов'язані з недостатнім захистом на стороні партнерів.

4. Аналіз впливу зовнішніх загроз - оцінка загроз, що походять від кіберзлочинців, хакерських атак, вірусних або шкідливих програм, а також ризиків, пов'язаних з природними катастрофами (повені, пожежі, техногенні аварії), які можуть порушити функціонування IT-систем.

5. Оцінка ефективності існуючих засобів захисту - періодична перевірка ефективності поточних засобів захисту інформаційних систем, таких як антивірусне програмне забезпечення, фаєрволи, системи виявлення вторгнень, а також перевірка їх на відповідність новим загрозам.

6. Аналіз впливу на репутацію та бізнес-процеси - оцінка ризиків, пов'язаних з порушенням інформаційної безпеки, і їх вплив на репутацію підприємства, а також можливі фінансові втрати та шкоду для бізнесу, що можуть виникнути через втрату довіри клієнтів або партнерів.

7. Оцінка відповідності законодавчим і нормативним вимогам - оцінка ризиків, пов'язаних з невідповідністю діючим стандартам та законодавчим вимогам у сфері інформаційної безпеки, таким як ISO/IEC 27001, GDPR, законодавство України щодо захисту персональних даних.

8. Оцінка впливу на технологічні процеси - оцінка ризиків, що можуть виникнути через порушення роботи інформаційних і автоматизованих систем виробництва (наприклад, збій у роботі системи управління виробничими процесами).

9. Підготовка та тестування плану реагування на інциденти - розробка плану дій на випадок інформаційного інциденту, перевірка його ефективності через регулярні тренування і симуляції реальних загроз.

Оцінка ризиків у корпоративній інформаційній безпеці для ПрАТ «Тернопільський молокозавод» повинна бути комплексною та включати

широкий спектр факторів, що стосуються як зовнішніх, так і внутрішніх загроз. Важливо визначити критичні для бізнесу інформаційні активи, оцінити всі можливі ризики, включаючи загрози з боку персоналу, партнерів та технологій, а також забезпечити ефективне реагування на інциденти для зниження їх впливу на виробничі процеси та репутацію підприємства.

Оцінка ризиків при впровадженні корпоративної інформаційної безпеки на ПрАТ «Тернопільський молокозавод» є ключовим етапом для забезпечення стабільної та безпечної роботи підприємства в умовах сучасних кіберзагроз та інформаційних атак. Враховуючи важливість захисту інформаційних активів для забезпечення безперервності виробничих процесів, збереження корпоративної репутації та дотримання нормативних вимог, необхідно систематично оцінювати потенційні ризики, що можуть вплинути на безпеку інформаційних систем підприємства.

Процес оцінки ризиків має включати кілька важливих етапів:

1. Ідентифікація та аналіз критичних інформаційних активів — важливо визначити найцінніші інформаційні ресурси підприємства, зокрема дані про клієнтів, фінансові операції, технологічні процеси та інтелектуальну власність, які потребують особливого захисту.

2. Виявлення і оцінка внутрішніх і зовнішніх загроз — необхідно оцінити як внутрішні загрози (помилки чи зловживання з боку персоналу), так і зовнішні (кібернапади, хакерські атаки, природні або техногенні катастрофи), які можуть порушити роботу інформаційних систем та призвести до витоку або втрати даних.

3. Розробка та впровадження політик безпеки — створення чітких регламентів і процедур для забезпечення належного захисту інформації, у тому числі доступу до неї, а також надання навичок і знань персоналу щодо безпечної роботи з корпоративними даними.

4. Використання сучасних технологічних засобів захисту — антивірусне ПЗ, фаєрволи, системи виявлення вторгнень та регулярне оновлення засобів захисту для відбиття новітніх загроз.

5. Моніторинг і реагування на інциденти — регулярний моніторинг інформаційних систем підприємства для своєчасного виявлення порушень безпеки та оперативного реагування на них. Це допоможе мінімізувати потенційні збитки і втрати від інцидентів.

6. Аналіз впливу на бізнес і репутацію — оцінка можливих фінансових та репутаційних втрат від інформаційних інцидентів, що можуть негативно вплинути на довіру клієнтів та партнерів.

7. Дотримання нормативно-правових вимог — відповідність діючим стандартам і вимогам у галузі інформаційної безпеки (ISO/IEC 27001, GDPR тощо) для забезпечення захисту персональних даних і відповідності законодавчим вимогам.

Завдяки ретельному та всебічному підходу до оцінки ризиків, ПрАТ «Тернопільський молокозавод» зможе не лише забезпечити безпеку своїх інформаційних систем, а й підвищити рівень довіри до підприємства з боку партнерів і клієнтів. Це дозволить мінімізувати можливі загрози та забезпечити стійкість і безперервність роботи заводу в умовах сучасних викликів кібербезпеки.

Висновки до розділу 2

Оцінка ризиків при впровадженні корпоративної інформаційної безпеки є невід'ємною частиною сучасного управління підприємствами, що прагнуть забезпечити стійкість своїх інформаційних систем, захист корпоративних даних і підтримання безперервності бізнес-процесів. У сучасному світі, де кіберзагрози постійно еволюціонують, ця оцінка стає критично важливою для запобігання втратам, витокам даних і порушенню довіри з боку партнерів і клієнтів.

Основні аспекти оцінки ризиків:

1. Ідентифікація загроз і вразливостей: необхідно розуміти як внутрішні (людський фактор, помилки працівників), так і зовнішні (хакерські атаки,

природні катастрофи) загрози для інформаційних систем підприємства. Виявлення таких ризиків є першим кроком до їх усунення.

2. Аналіз потенційного впливу на бізнес: оцінка того, які наслідки матимуть інциденти з інформаційною безпекою для фінансових і репутаційних аспектів діяльності підприємства. Це дозволяє створити пріоритети у впровадженні заходів безпеки.

3. Впровадження політики безпеки та технічних засобів захисту: розробка чітких регламентів і процедур для збереження конфіденційності, цілісності та доступності даних є основою захисту. Технічні засоби (антивірусне ПЗ, фаєрволи, системи моніторингу) мають стати невід'ємною частиною цієї політики.

4. Навчання персоналу і підвищення обізнаності: важливо, щоб кожен співробітник розумів свою роль у забезпеченні інформаційної безпеки і мав необхідні навички для запобігання інцидентам безпеки. Тренінги та сертифікація є важливою складовою системи захисту.

5. Моніторинг і реагування на інциденти: постійний контроль за станом безпеки дозволяє швидко виявляти та реагувати на порушення, мінімізуючи їх негативні наслідки.

6. Відповідність нормативним вимогам: дотримання стандартів і вимог законодавства (ISO/IEC 27001, GDPR) допомагає не лише захистити інформацію, а й уникнути юридичних та фінансових санкцій.

Оцінка ризиків при впровадженні корпоративної інформаційної безпеки є критично важливою для захисту підприємства від численних загроз. Це дозволяє не лише зберегти конфіденційність і цілісність даних, а й підтримувати безперервність бізнесу, зберігати репутацію та конкурентоспроможність на ринку. За допомогою систематичної оцінки ризиків та впровадження відповідних заходів безпеки організації можуть ефективно реагувати на нові виклики в сфері інформаційної безпеки, забезпечуючи стабільність і розвиток у довгостроковій перспективі.

РОЗДІЛ 3.
ШЛЯХИ ЗНИЖЕННЯ РИЗИКІВ ПРИ ВПРОВАДЖЕННІ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Алгорітм оцінки і управління ризиками при впровадженні корпоративної інформаційної безпеки

Алгоритм оцінки ефективності заходів щодо мінімізації наслідків ризиків впровадження корпоративної інформаційної безпеки (КІБ) на передінвестиційній стадії включає такі етапи:

1. Ідентифікація критичних змінних ризиків, які можуть суттєво вплинути на забезпечення корпоративної інформаційної безпеки.

2. Визначення характеристик і параметрів критичних змінних ризиків, таких як ймовірність їх настання, ступінь впливу та взаємозв'язки.

3. Розрахунок витрат на компенсацію змін критичних змінних ризиків за визначеною формулою (3).

4. Оцінка очікуваного впливу критичних змінних ризиків на загальні витрати проекту КІБ із застосуванням формули (4).

5. Вибір стратегії адаптації інвестиційного проекту до змін критичних змінних ризиків, спираючись на результати попередніх розрахунків.

6. Обчислення загального бюджету для компенсації ризиків, який враховує витрати на компенсацію змін усіх критичних змінних ризиків проекту КІБ.

7. Розрахунок критеріїв ефективності інвестування з урахуванням наслідків ризиків для проекту забезпечення корпоративної інформаційної безпеки.

Цей алгоритм сприяє системній оцінці ризиків у сфері інформаційної безпеки та оптимізації витрат для їх мінімізації.

Витрати на компенсацію зміни критичної змінної запропоновано обчислювати за формулою $БКР_i = \left(\frac{V_{maxi}}{V_{ni}} - 1 \right) * C_i$, (4)

де БКРі - витрати на компенсацію зміни критичної змінної ризику і, грн., Vmaxi - найбільш ймовірне значення критичної змінної і, од.,Vпі - порогове значення критичної змінної і, од., Сі - витрати на зниження поточного значення критичної змінної і на один відсоток, грн./%.

Розрахунок величини очікуваного впливу на витрати по проекту КІС окремих критичних змінних ризику запропоновано здійснювати за формулою

$$ОВ_i = \frac{БКР_i}{\sum_{(j)} \alpha_j} * \alpha_i, \quad (5)$$

де ОВі - величина очікуваного впливу на витрати по проекту критичної змінної і, грн., *а*і - ваговий коефіцієнт критичної змінної і, од. Вагові коефіцієнти, що визначають значимість критичних змінних, визначаються експертними методами.

Зіставляючи витрати на компенсацію зміни критичної змінної та очікуваний вплив цієї змінної ризику, можна обрати найбільш економічно вигідний спосіб реагування на ризик.

Алгоритм оцінки ефективності заходів для зменшення наслідків ризиків дає змогу зіставити ризики з економічною доцільністю впровадження корпоративної інформаційної безпеки (КІБ) шляхом нормування значень ключових змінних (NPV ≥ 0). Цей алгоритм сприяє вибору оптимальної стратегії адаптації інвестиційного проєкту до впливу ризиків.

На рисунку 3.1. представлено алгоритм управління ризиками інвестування в корпоративну інформаційну безпеку (КІБ), який включає сукупність управлінських процесів, спрямованих на контроль бюджету, забезпечення економічної ефективності, дотримання календарного плану, а також комплекс заходів з ідентифікації, оцінки та мінімізації ризиків на кожному етапі реалізації інвестиційного проєкту у сфері КІБ.

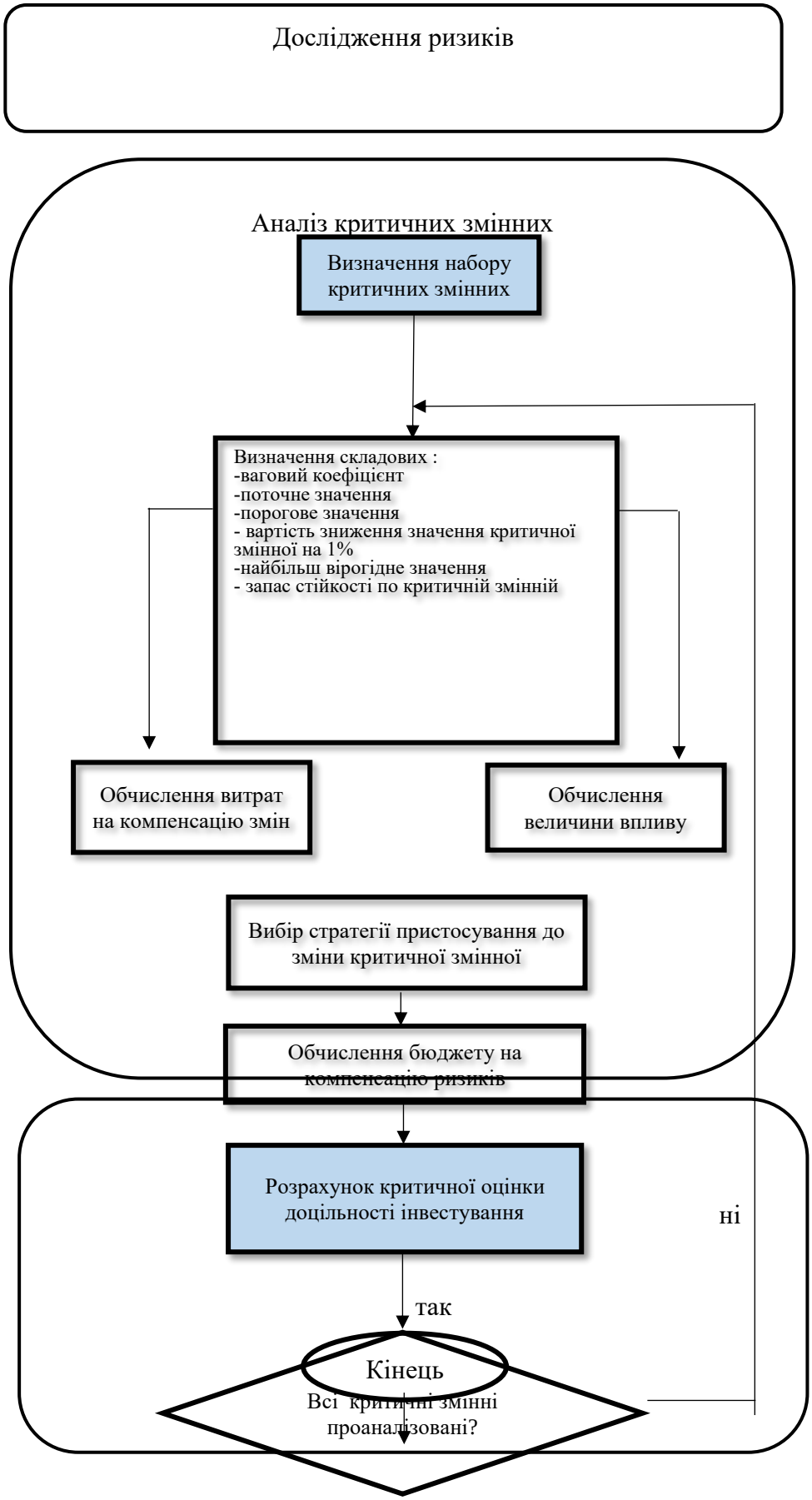

Рис.3.1 Алгоритм оцінки ефективності засобів для мінімізації наслідків ризиків впровадження КІБ.

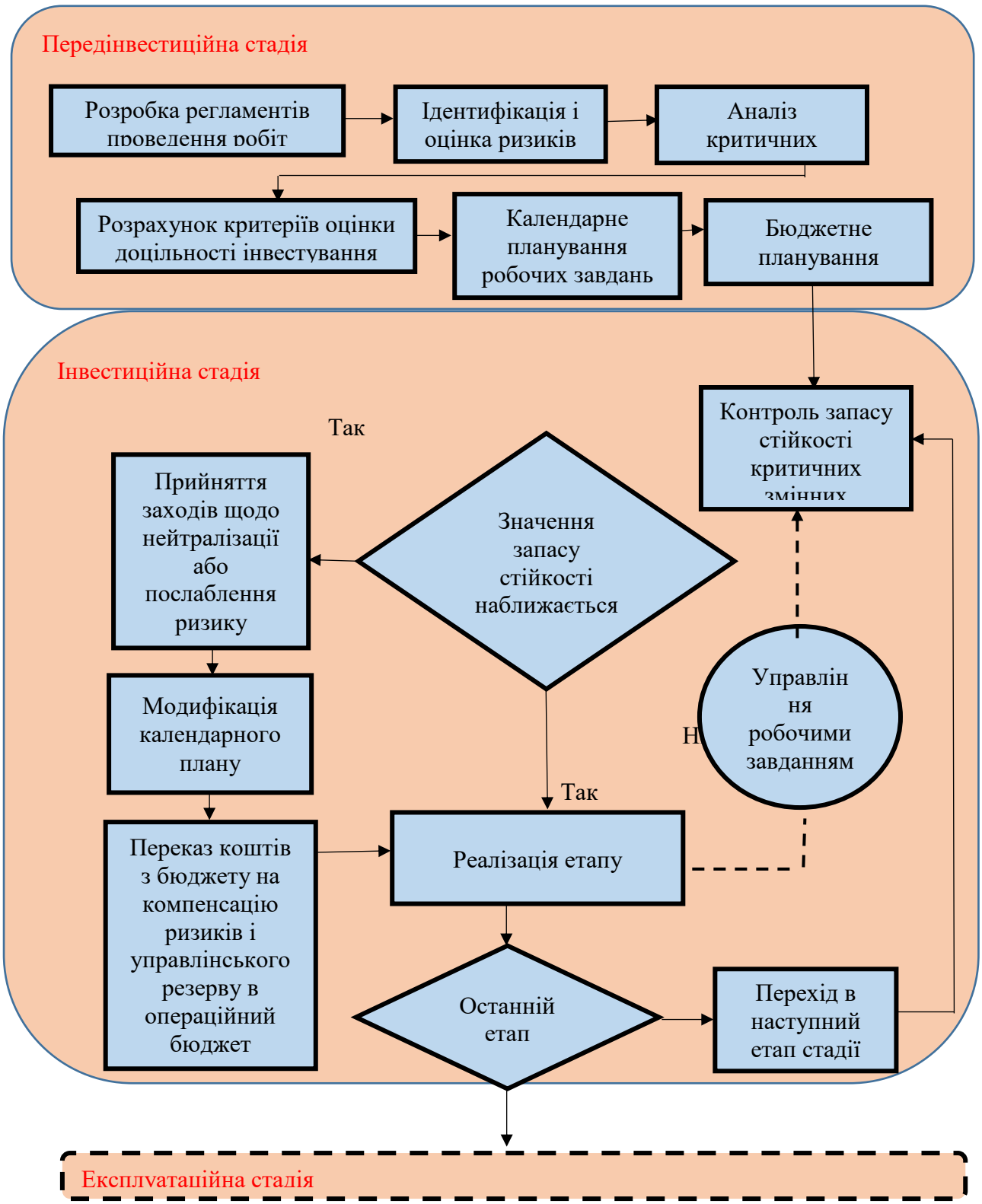

Рис.3.2 Алгоритм управління ризиками при впровадженні КІБ

На наш погляд, прогнозування ризиків та врахування наслідків їх реалізації є ключовою метою передінвестиційної стадії проєкту впровадження корпоративної інформаційної безпеки (КІБ). Для досягнення цієї мети важливо

вирішити завдання, пов’язані з розробкою регламентів виконання проєктних робіт, ідентифікацією та оцінкою ризиків, а також аналізом критично важливих змінних.

На наш погляд, основною метою інвестиційної стадії проєктів впровадження корпоративної інформаційної безпеки (КІБ) є моніторинг запасу стійкості критично важливих змінних для своєчасного вжиття заходів з нейтралізації або зменшення впливу ризиків. Цей контроль здійснюється в межах процесу управління ризиками на кожному етапі реалізації проєкту впровадження КІБ.

Для більш детального вивчення корпоративної інформаційної безпеки та оцінки ризиків на ПрАТ «Тернопільський молокозавод» можна провести SWOT – аналіз (табл.3.1.). Цей аналіз допомагає визначити пріоритети для покращення корпоративної інформаційної безпеки та підготовки до різних ризиків, зокрема тих, що виникають у зв'язку з війною та економічною ситуацією в країні.

Таблиця 3.1.

SWOT – аналіз корпоративної інформаційної безпеки та оцінки ризиків на ПрАТ «Тернопільський молокозавод»

Сильні сторони	**Слабкі сторони**
Стабільна репутація на ринку Модернізоване обладнання Лояльність клієнтів Наявність сертифікатів якості та безпеки Високий рівень автоматизації та впровадження ІТ-технологій	Залежність від зовнішніх постачальників сировини Висока енергоємність виробництва Слабка диверсифікація ринку Застаріле програмне забезпечення
Можливості	**Загрози**
Експансія на міжнародні ринки Інвестиції в інновації та нові продукти Розвиток інфраструктури корпоративної інформаційної безпеки Державні програми підтримки	Війна та геополітична нестабільність Кіберзагрози Коливання цін на сировину та енергоносії Конкуренція з боку імпортерів Ризик несанкціонованого доступу до інформації**:**

Охарактеризуємо їх більш детально:

1. Сильні сторони (Strengths)

- **Стабільна репутація на ринку**: Завод має сильну позицію на українському ринку молочної продукції завдяки багаторічному досвіду та відомому бренду.
- **Модернізоване обладнання**: Постійні інвестиції в модернізацію технологічного обладнання дозволяють забезпечити високу якість продукції та ефективність виробництва.
- **Лояльність клієнтів**: Висока лояльність споживачів, завдяки сталому якості продукції та бренду.
- **Наявність сертифікатів якості та безпеки**: Сертифікація відповідно до міжнародних стандартів якості (ISO, HACCP тощо).
- **Високий рівень автоматизації та впровадження IT-технологій**: Розвинена система корпоративної інформаційної безпеки, використання сучасних програмних засобів для управління бізнес-процесами, що знижує ризики інформаційних атак.

2. Слабкі сторони (Weaknesses)

- **Залежність від зовнішніх постачальників сировини**: Переривання постачань молока або інших сировинних компонентів через геополітичну ситуацію або нестабільність в постачаннях можуть призвести до перебоїв у виробництві.
- **Висока енергоємність виробництва**: Зростання цін на енергоносії може негативно вплинути на собівартість продукції та знизити конкурентоспроможність.
- **Слабка диверсифікація ринку**: Оскільки основна частина продажів припадає на внутрішній ринок, завод може стикатися з обмеженням можливостей для зростання через економічну нестабільність та війну.
- **Застаріле програмне забезпечення**: Незважаючи на загальну автоматизацію, можливо, не всі програмні рішення є сучасними або достатньо захищеними від кібератак.

3. Можливості (Opportunities)

- **Експансія на міжнародні ринки**: Розширення на нові ринки, зокрема ЄС та інші країни, може допомогти зменшити залежність від внутрішнього ринку, знизити ризики від війни та економічної нестабільності.
- **Інвестиції в інновації та нові продукти**: Випуск нових видів продукції (наприклад, безлактозні або органічні молочні продукти) може допомогти залучити нових споживачів та створити додаткові джерела доходу.
- **Розвиток інфраструктури корпоративної інформаційної безпеки**: Впровадження новітніх технологій для захисту інформації від кібератак, що є особливо важливим у часи війни. Можливість застосування систем штучного інтелекту для прогнозування ризиків та оптимізації виробничих процесів.
- **Державні програми підтримки**: Уряд може запровадити програми підтримки агропромислових підприємств, що дозволить зменшити вплив економічних і політичних ризиків.

4. Загрози (Threats)

- **Війна та геополітична нестабільність**: Війна в Україні створює великі ризики для логістики, безпеки виробництва, а також може призвести до втрат через руйнування інфраструктури чи обмеження постачання.
- **Кіберзагрози**: Акти кібертероризму або злам системи корпоративної інформаційної безпеки можуть призвести до втрати даних, зупинки виробництва або фінансових збитків.
- **Коливання цін на сировину та енергоносії**: Вплив глобальних економічних факторів, таких як зростання вартості енергоресурсів або нестабільність на ринку молочної сировини, можуть призвести до підвищення витрат.
- **Конкуренція з боку імпортерів**: Зниження імпортних бар'єрів або дешевші імпортовані товари можуть призвести до зменшення попиту на українську молочну продукцію.

- **Ризик несанкціонованого доступу до інформації**: Оскільки завод може працювати з великими обсягами конфіденційних даних, витік інформації чи неправомірний доступ до баз даних може стати серйозною загрозою для компанії.

Таким чином, алгоритм оцінки і управління ризиками при впровадженні корпоративної інформаційної безпеки має на меті комплексно охопити всі аспекти інформаційної безпеки, починаючи від ідентифікації загроз і закінчуючи моніторингом і навчанням персоналу. Впровадження ефективної стратегії управління ризиками дозволяє мінімізувати можливі збитки від кібератак, природних чи техногенних катастроф, а також гарантує постійну готовність організації до реагування на нові загрози.

Ключові компоненти успішного управління ризиками:

1. Систематична оцінка та аналіз ризиків.
2. Вибір адекватних стратегій для управління ними.
3. Постійний моніторинг і адаптація до змін у загрозах.
4. Навчання персоналу та створення культури безпеки.

Імплементація цього алгоритму в організаційну практику дозволяє не тільки захистити корпоративну інформацію, а й забезпечити стабільну і безпечну діяльність підприємства в умовах сучасних інформаційних викликів.

3.2. Розробка моделі для оцінки ефективності корпоративної інформаційної безпеки.

Впровадження та експлуатація корпоративних інформаційних систем супроводжуються ризиками, зумовленими наявністю низки непередбачуваних факторів невизначеності. Проект впровадження корпоративної інформаційної безпеки (КІБ) включає кілька етапів, що виконуються як послідовно, так і паралельно; результати кожного етапу впливають на загальну реалізацію системи та на подальші етапи. Отже, негативні наслідки прояву ризиків у

процесі реалізації інвестицій можуть виникати неодноразово, що збільшує загальні втрати від їх прояву.

Аналіз літературних джерел не виявив єдиної загальноприйнятої методології оцінки ефективності інвестування в інформаційні технології (ІТ). Тому ми спробували формалізувати цей процес, розробивши модель для оцінки ефективності інвестування в ІТ.

Модель дозволяє розподіляти проект на логічні етапи та оперативно отримувати результати. Таким чином, можна швидко створити сховище даних та забезпечити випуск базових звітних форм, а згодом поступово розширювати обсяг даних, що збираються в сховище, і допрацьовувати функціональність для генерації складніших звітів. Ця модель допоможе реалістично оцінити терміни виконання кожного етапу ІТ-проекту.

Крім того, застосування моделі сприяє побудові проекту відповідно до бізнес-цілей підприємства, дозволяючи структурувати його за ключовими бізнес-напрямками.

Для впровадження моделі оцінки ефективності ІТ-проекту необхідно визначити:

- показники комерційної ефективності, що враховують фінансові наслідки реалізації проекту для безпосередніх учасників;

- показники бюджетної ефективності, які відображають фінансові наслідки проекту для бюджетів різних рівнів;

- показники економічної ефективності, що враховують результати та витрати, пов'язані з реалізацією інвестиційного проекту, які виходять за межі інтересів учасників і допускають вартісне вимірювання.

Для оцінки ефективності проекту автоматизації потрібно розглянути два стани системи управління.

Перший стан, початковий, відображає поточний стан на момент часу (стан «як є»), коли проект ще не розпочався. Початковий стан визначається набором показників ефективності системи управління та їх унікальними

значеннями. Важливим аспектом є наявність функціонуючої на підприємстві збалансованої системи показників.

Другий стан, кінцевий, визначає ситуацію після завершення передбаченого проекту (стан «як повинно бути»). Він включає той самий набір показників ефективності, що й початковий стан. Інакше кажучи, в процесі реалізації проекту відбуваються зміни в показниках ефективності, що дозволяє наблизитися до досягнення встановлених цілей, які характеризуються конкретними значеннями цих показників.

Подальший аналіз ефекту від автоматизації може здійснюватися різними методами. Можна порівняти різницю між значеннями показників ефективності кінцевого і початкового стану, або оцінити, наскільки підприємство наблизилося до досягнення запланованих цільових значень показників ефективності в результаті проекту. Інший підхід — це аналіз відхилень фактично досягнутих значень показників ефективності від запланованих (план-фактичний аналіз).

З точки зору кінцевих бізнес-ефектів, на найвищому рівні оцінки потенційних економічних вигод виділяються загальні, важливі напрямки, які визначають економічну ефективність будь-яких інвестицій, що отримали назву ключових факторів економічної ефективності [3,5]:

- мінімізація упущеного доходу або створення нових джерел доходів;
- зменшення поточних виробничих (експлуатаційних) витрат;
- скорочення адміністративно-управлінських витрат;
- мінімізація податкових та інших обов'язкових платежів;
- зменшення штрафних санкцій та інших позареалізаційних витрат;
- зниження потреби в капітальних витратах;
- підвищення оборотності поточних активів.

Як інтегральний показник доходної частини інвестиційного проекту з впровадження інформаційних технологій для оцінки комерційної ефективності проекту доцільно використовувати сумарний грошовий потік, виражений через чистий дохід, що залишається в розпорядженні організації.

Цей показник є комплексним вираженням всіх значущих ефектів, які забезпечуються реалізацією проекту. На основі цього для замовника (інвестора) можна здійснити розрахунок будь-якого показника ефективності (ROI, NPV, IRR, PP тощо).

Основною складністю при оцінці результативності інвестицій в IT-проекти є обмежена здатність фінансових методів оцінки, оскільки необхідно враховувати нефінансові вигоди IT-проекту.

Економічна ефективність впровадження інформаційної системи в компанії може визначатися через:

- різницю між заявленою та реальною трудомісткістю виконання робіт;

- економію ресурсів (зниження простоїв персоналу, оптимізацію використання матеріальних запасів) завдяки удосконаленню процесу забезпечення ресурсами;

- зміну швидкості виконання завдань при тих самих ресурсах;

- більш оперативну реакцію на події;

- підвищення інвестиційної привабливості через більш строгий контроль за використанням ресурсів;

- збільшення мотивації працівників;

- покращення обчислювальних можливостей для обробки великих обсягів даних;

- повніше використання бізнес-можливостей завдяки моніторингу зовнішнього середовища та ефективності процесів.

Ефективність інформаційної системи залежить від її наповнення та якості реалізації, тобто результат впровадження ІС визначається якістю бізнес-моделі.

Принципи економічної ефективності компанії потрібно перевести в конкретні показники для оцінки її економічної ефективності. Для цього визначаються вимоги до системи оцінки економічної ефективності компанії:

1. Система показників повинна включати як фінансові, так і нефінансові показники, при цьому між ними має бути взаємозв'язок, а також взаємозв'язок

з організаційними рівнями в компанії. Кількість показників має бути обмеженою, щоб забезпечити своєчасну оцінку і прийняття рішень.

2. Система показників повинна враховувати як минуле, так і поточний стан бізнесу.

3. Показники мають бути корисними для прогнозування майбутнього компанії, зокрема для оцінки її вартості або капіталізації, приросту обсягу продажів і виручки.

4. Система показників повинна бути пов'язана зі стратегією компанії та її стратегічними цілями. Зміна стратегії може вимагати коригування як значень показників ефективності, так і самої системи.

5. Система показників повинна враховувати інтереси та потреби зацікавлених сторін, таких як акціонери, вищий керівний склад, споживачі тощо.

6. Система показників повинна бути значущою, адекватною, послідовною та стабільною, тобто вона повинна мати логічну послідовність змін, що дозволяє співробітникам компанії відслідковувати зміни і адаптуватися до них. Короткострокові показники повинні бути узгоджені з довгостроковими.

7. Впровадження системи показників не повинно ускладнювати доступність інформації для розрахунків і призводити до значних додаткових витрат.

Аналіз джерел META Group, Gartner Group, ISM дозволив виділити основні категорії ефектів від впровадження ІБ (рис 3.3).

На функціональному рівні предметом вимірювання є внесок IT у виконання функцій структурними підрозділами, при цьому зібрана інформація використовується для підвищення ефективності внутрішніх процесів. На цьому рівні здійснюється аналіз даних про ефективність проектів і програм, а також їх подання вищому керівництву організації.

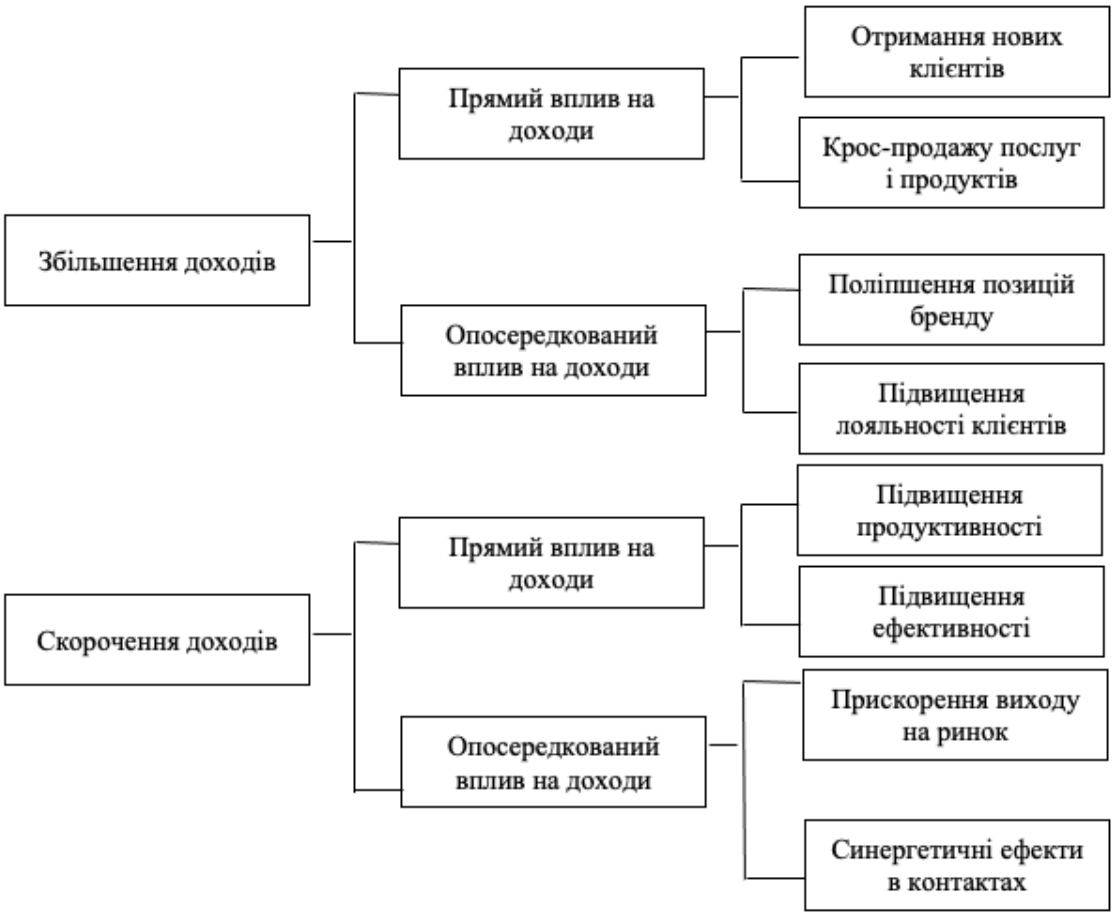

Рис.3.3 - Основні категорії ефектів від впровадження ІБ

Модель оцінки економічної ефективності включає ієрархічне представлення показників ефективності, які відображають умови зовнішнього та внутрішнього середовища компанії. В рамках цієї моделі визначаються показники, виконання яких є критичним для досягнення стратегічних цілей досліджуваної компанії.

Таким чином, використання запропонованої моделі оцінки ефективності корпоративної інформаційної безпеки (КІБ) дозволяє значно покращити фінансові результати проекту впровадження.

3.3 Шляхи покращення ефективності впровадження корпоративних інформаційних систем на ПрАТ «Тернопільський молокозавод»

Залежно від розміру підприємства, системи управління можна умовно поділити на два основні класи. Великі системи, які повністю відповідають

вимогам стандарту ERP, являють собою великі інтегровані комплекси, що, окрім інструментів для управління виробництвом, включають додаткові модулі, що значно розширюють можливості традиційних ERP-систем, наприклад, CRM, ASP, OLAP. Оскільки не кожне підприємство має достатньо ресурсів для впровадження таких систем, для них зазвичай використовуються середні системи, наближені до стандарту ERP. Ці системи включають різноманітні інструменти для автоматизації бухгалтерського обліку, управління персоналом, організації документообігу, складського обліку, фінансового аналізу, бізнес-планування та технологічної підтримки виробництва. Для забезпечення ефективного управління ІБ нами були систематизовані основні характеристики ІБ (табл. 3.2).

Таблиця 3.2.

Основні характеристики корпоративної інформаційної безпеки

Назва характеристики	Сутність
Конфіденційність	Це характеристика, яка забезпечує доступ до інформації лише тим особам або системам, які мають на це право. Конфіденційність передбачає захист даних від несанкціонованого доступу, що включає як внутрішні, так і зовнішні загрози.
Цілісність	Цілісність даних гарантує, що інформація не буде змінена або знищена без належного дозволу. Вона також означає, що дані не можуть бути випадково або навмисно змінені, порушуючи їх достовірність.
Доступність	Ця характеристика забезпечує доступ до інформації та інформаційних систем у будь-який час, коли це необхідно для авторизованих користувачів. Це включає збереження працездатності інфраструктури, зокрема резервних копій та систем відновлення після збоїв.
Аутентифікація та авторизація	Процеси аутентифікації та авторизації дозволяють перевірити ідентичність користувачів або систем, а також визначити їх права доступу до конкретної інформації або ресурсів.

Моніторинг та аудит	Постійний моніторинг систем на предмет виявлення аномальних подій або несанкціонованих спроб доступу. Аудит дозволяє відстежувати, хто, коли та які зміни вносив в систему, що важливо для виявлення і реагування на загрози.
Управління ризиками	Постійна оцінка потенційних загроз для інформаційних систем та вжиття заходів для мінімізації цих ризиків. Це включає виявлення вразливих місць і впровадження необхідних контрзаходів для їх усунення.
Інцидент-менеджмент	Процес реагування на інциденти безпеки, включаючи виявлення, оцінку, реагування та відновлення після інциденту, що може включати крадіжку даних, атаки на систему або будь-які інші порушення безпеки
Підготовка та навчання персоналу	Постійне навчання співробітників компанії щодо політик безпеки, методів захисту інформації, а також актуальних загроз. Це важливо для зменшення людського фактора у виникненні інцидентів безпеки.
Забезпечення відповідності	Відповідність нормативним вимогам і стандартам безпеки, таким як GDPR, ISO/IEC 27001, або галузевим регулюванням. Це включає впровадження політик та процедур, які відповідають вимогам законодавства і знижують юридичні та фінансові ризики.
Безпека програмного забезпечення та мережі	Це включає захист інформаційних систем від уразливостей програмного забезпечення, використання антивірусних та антишпигунських засобів, шифрування даних, використання захищених каналів зв'язку та безпеки на рівні мережевих пристроїв.
Резервне копіювання та відновлення	Створення регулярних резервних копій критичної інформації та планування процесів відновлення систем у разі збою, щоб забезпечити безперервність бізнесу.

Ці характеристики разом визначають надійність і ефективність корпоративної інформаційної безпеки, дозволяючи організації мінімізувати можливі загрози та зберегти цінні дані в умовах постійної цифрової еволюції.

Таким чином, побудова корпоративної системи управління інформаційною безпекою з урахуванням її основних характеристик повинна відповідати масштабам та специфіці діяльності підприємства. Якщо інформаційна безпека не відповідає цим вимогам, її впровадження не дасть очікуваного результату: комп'ютеризованими стануть лише окремі ділянки управління, без належного взаємозв'язку та взаємообумовленості. Оскільки корпоративні інформаційні системи є інтегрованими системами управління, це означає, що:

- ці системи не є безпосередньо пов'язаними з виробничими процесами та не автоматизують управління технологічними процесами, а працюють з моделями цих процесів;

- їхня діяльність спрямована на поліпшення функціонування підприємства, оптимізацію матеріальних і фінансових потоків на основі інформації, що вводиться на робочих місцях;

- в одній системі охоплюється планування та управління усією діяльністю виробничого підприємства, від закупівлі сировини до відвантаження товару споживачеві;

- інформація вводиться в систему лише один раз у тому підрозділі, де вона виникає, зберігається в одному місці і використовується кількома підрозділами, що мають до неї доступ.

Корпоративна інформаційна безпека дозволяє вирішувати такі завдання: організувати ефективне планування всіх фінансових та господарських процесів; збільшити довіру інвесторів через забезпечення максимальної прозорості бізнесу; знизити ризики та підвищити прибутковість завдяки швидкому та точному прийняттю рішень, інтуїтивно зрозумілій системі управління, чітким обмеженням доступу до інформації за посадовими функціями співробітників і забезпеченню її безпеки; зменшити втрати часу

завдяки усуненню дублювання даних різними службами і налагодженню безперешкодного обміну інформацією між підрозділами компанії.

Таким чином, системи цього класу забезпечують узгоджену роботу різних підрозділів, що сприяє зниженню адміністративних витрат і вирішенню проблеми інтеграції даних для різних додатків. Вони є потужним інструментом для підвищення ефективності управління, сприяючи прийняттю обґрунтованих стратегічних і тактичних рішень на основі своєчасної та достовірної інформації. Впровадження корпоративних систем дозволяє здобути конкурентні переваги шляхом оптимізації бізнес-процесів та зниження витрат.

Для ефективного впровадження корпоративної інформаційної безпеки на ПрАТ «Тернопільський молокозавод» можна виділити кілька ключових проблемних аспектів, які потребують уваги та детального розгляду (табл. 3.3).

Таблиця 3.3.

Проблемні аспекти ефективного впровадження корпоративної інформаційної безпеки на ПрАТ «Тернопільський молокозавод»

Проблемні аспекти	Характеристика
Низький рівень обізнаності співробітників	Впровадження корпоративної інформаційної безпеки потребує участі всіх співробітників, включаючи тих, хто не є безпосередньо залученим до IT-процесів. Низький рівень обізнаності працівників щодо важливості інформаційної безпеки може призвести до порушень політик безпеки та витоку конфіденційної інформації. Для вирішення цього питання необхідно провести навчання та тренінги для персоналу.
Інтеграція систем безпеки з існуючими IT-інфраструктурами	В умовах наявної IT-інфраструктури підприємства можуть виникнути труднощі при інтеграції нових рішень для інформаційної безпеки з вже діючими системами, такими як ERP-системи, управлінські програми, бази даних тощо. Це потребує ретельного планування та можливого оновлення або адаптації існуючих технологій для забезпечення належного рівня захисту.

Нестабільність фінансування та ресурсів	Однією з основних проблем є недостатнє фінансування для повноцінного впровадження та підтримки систем безпеки на всіх етапах роботи підприємства. Відсутність належних ресурсів може затримати впровадження необхідних інструментів для забезпечення корпоративної безпеки або обмежити масштаби впровадження.
Культурні та організаційні бар'єри	Проблемою для успішного впровадження корпоративної інформаційної безпеки є відсутність в організації культури безпеки, а також можлива опірність змінам з боку працівників, які звикли до традиційних методів роботи. Це може стати серйозною перешкодою на шляху до реалізації проекту. Для цього необхідно забезпечити підтримку керівництва, яке повинно активно демонструвати важливість інформаційної безпеки.
Аналіз ризиків і визначення вразливостей	Перед впровадженням інформаційної безпеки необхідно провести глибокий аналіз потенційних загроз і вразливостей в існуючих інформаційних системах підприємства. Невизначеність щодо реальних загроз та недостатньо точне оцінювання ризиків можуть призвести до неповної чи неефективної реалізації заходів безпеки.
Низька гнучкість системи безпеки	Потреба у регулярному оновленні політик та систем захисту може бути ускладнена відсутністю гнучких інструментів для адаптації до нових умов або змін у бізнес-процесах. Це може бути проблемою для молокозаводу, де швидко змінюються вимоги ринку та технології виробництва. Рішення для цього питання можуть включати впровадження гнучких, масштабованих рішень, які можна адаптувати до майбутніх потреб.
Моніторинг та управління безпекою	Проблемою може стати також недостатній рівень моніторингу та управління системою безпеки після її впровадження. Регулярний моніторинг необхідний для своєчасного виявлення та усунення інцидентів безпеки. Без належного контролю система може стати вразливою до зовнішніх та внутрішніх загроз.
Забезпечення відповідності законодавчим вимогам	Важливо також врахувати необхідність дотримання законодавчих та нормативних вимог щодо захисту даних і інформації. Це особливо актуально для підприємства, яке

	працює в харчовій галузі, де існують специфічні вимоги щодо захисту інформації та контролю за її обробкою. Затримки у виконанні таких вимог можуть призвести до юридичних наслідків для компанії.

Розглянувши проблемні аспекти, можна запропонувати наступні шляхи вирішення проблем:

- Проведення внутрішніх тренінгів та серій навчальних курсів для співробітників з усіх рівнів.
- Вибір надійних, інтегрованих систем для захисту даних та їх адаптація до поточної інфраструктури.
- Планування та забезпечення достатнього фінансування на всіх етапах проекту впровадження інформаційної безпеки.
- Формування організаційної культури безпеки через активну підтримку керівництва та залучення всіх співробітників.
- Регулярний аудит та оцінка ризиків, а також постійне вдосконалення заходів безпеки.
- Впровадження систем моніторингу та постійного оновлення програмного забезпечення для забезпечення максимальної безпеки.

Ці заходи дозволять ПрАТ «Тернопільський молокозавод» забезпечити належний рівень інформаційної безпеки та знизити потенційні ризики в процесі впровадження.

Враховуючи тему роботу, на нашу думку, є необхідним сформувати вимоги до уточненого критерію ефективності впровадження КІБ саме для ПрАТ «Тернопільський молокозавод», які відображені на рис.3.4.

Отже, визначені критерії повинні охоплювати три основні категорії характеристик корпоративної інформаційної безпеки: економічні, що включають фінансові та ресурсні критерії; функціональні, до яких належать якісні, часові характеристики та надійність виконання інформаційних процесів; а також соціальні критерії. При виборі системи ці критерії повинні

розглядатися в комплексі, що гарантує правильність та ефективність прийнятого рішення.

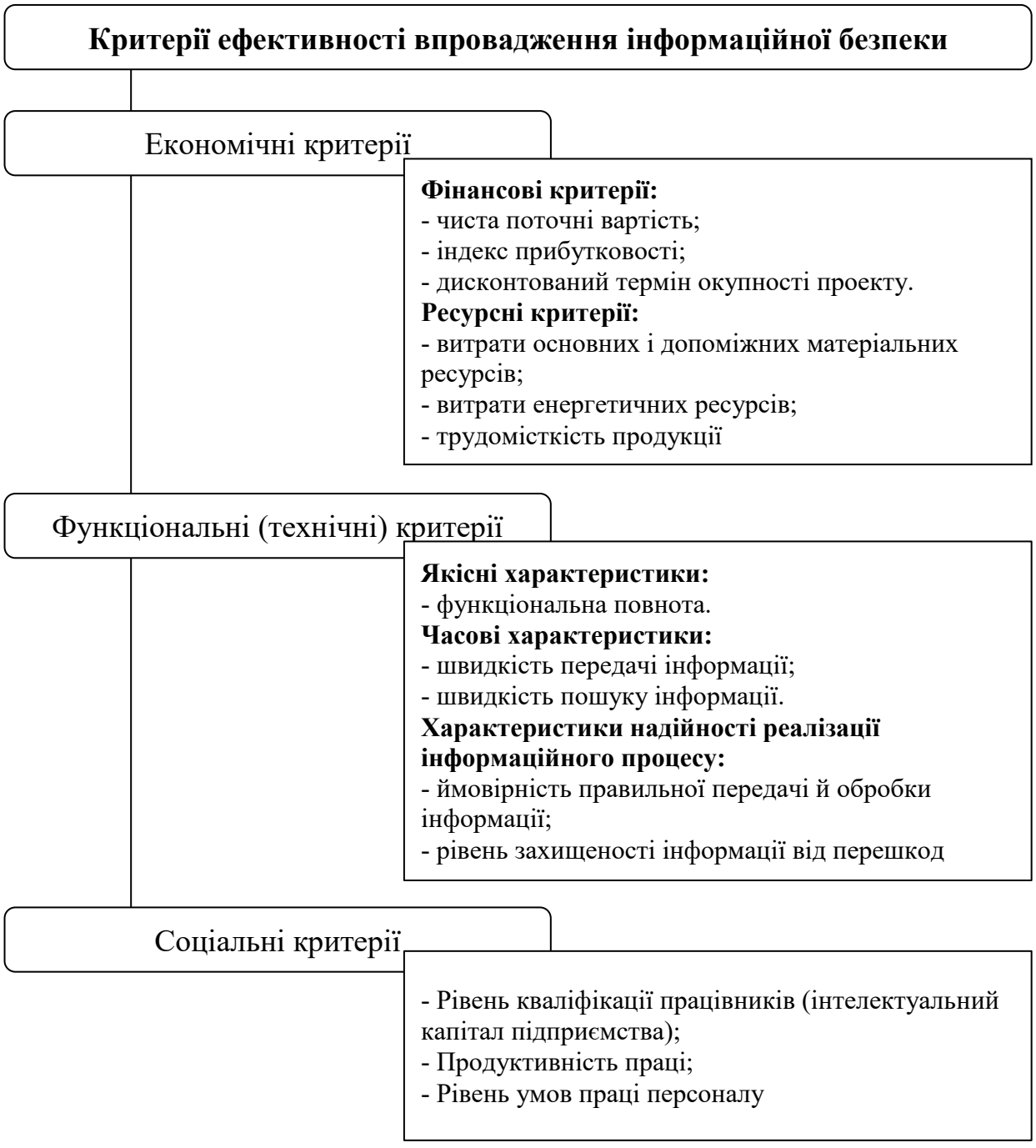

Рисунок 3.4. - Вимоги до уточненого критерію ефективності (оптимальності) впровадження інформаційної безпеки для ПрАТ «Тернопільський молокозавод»

Необхідно враховувати, що ефект від впровадження може бути як кількісно виміряним, так і не піддаватися точному обчисленню. До можливих факторів, що визначають загальний ефект від автоматизації, належать:

- покращення якості та скорочення часу процесів підготовки і прийняття рішень;
- оптимізація виробничої програми підприємства;
- визначення оптимальних рівнів запасів матеріальних ресурсів і обсягів незавершеного виробництва;
- скорочення часу оборотності оборотних коштів;
- стандартизація бізнес-процесів у всіх підрозділах підприємства, узгодження звітності за результатами діяльності різних підрозділів до єдиного стандарту;
- зниження трудомісткості обробки та використання даних, перепрофілювання персоналу, звільнення від рутинних завдань та перехід до більш інтелектуальних видів діяльності, що, в свою чергу, призводить до скорочення штату та збільшення продуктивності праці.

Застосування інформаційної безпеки для управління підприємством підвищує його конкурентоспроможність завдяки покращеній керованості та здатності швидко адаптуватися до змін ринкової ситуації. Створення корпоративної інформаційної безпеки в управлінні корпораціями, враховуючи її ключові характеристики (масштабність, багатоплатформність, розподілені обчислення та робота в неоднорідному середовищі), буде залежати від розмірів та специфіки діяльності конкретної корпорації.

Висновки до розділу 3

Впровадження корпоративної інформаційної безпеки (КІБ) є критично важливим етапом для забезпечення стабільності та ефективності функціонування підприємств у сучасних умовах. Для зниження ризиків при впровадженні КІБ необхідно враховувати кілька ключових факторів:

1. Забезпечення комплексного підходу до впровадження. Це включає не лише технічну, але й організаційну підготовку, створення відповідних внутрішніх політик та процедур, що дозволяють ефективно керувати ризиками на всіх етапах проекту.

2. Оцінка та управління ризиками на кожному етапі реалізації. Систематичне оцінювання потенційних загроз та визначення заходів для їх мінімізації дозволяє знизити ймовірність негативних наслідків від впровадження КІБ.

3. Покращення навчання та підготовки персоналу. Оскільки основною проблемою для багатьох підприємств є недостатня кваліфікація співробітників, важливо забезпечити належне навчання з питань інформаційної безпеки для всіх рівнів персоналу.

4. Адаптація до змін у технологічному середовищі. Врахування новітніх тенденцій в інформаційних технологіях і забезпечення гнучкості у системі КІБ дозволяє знижувати ризики, пов'язані з застарілими технологіями або змінами в законодавстві.

5. Моніторинг та регулярні перевірки. Постійний моніторинг ефективності системи КІБ та її адаптація до змін бізнес-процесів або зовнішніх умов є важливими інструментами для зниження ризиків і підтримки високого рівня безпеки.

Таким чином, зниження ризиків при впровадженні корпоративної інформаційної безпеки передбачає всебічний підхід, що включає технічні, організаційні та людські аспекти. Задля успішної реалізації важливо забезпечити належну координацію між усіма учасниками процесу та своєчасне реагування на зміну умов зовнішнього та внутрішнього середовища підприємства.

ВИСНОВОК

Розробка та впровадження корпоративних інформаційних систем є важливим етапом у розвитку організацій, що прагнуть до оптимізації своїх бізнес-процесів і забезпечення ефективного управління. Теоретичні основи цієї діяльності включають вивчення різних підходів до проектування, інтеграції та використання інформаційних систем, які відповідають специфічним потребам організації та сприяють її розвитку.

1. Роль корпоративних інформаційних систем полягає в автоматизації та інтеграції ключових бізнес-процесів, що дозволяє підвищити продуктивність, зменшити витрати та поліпшити контроль за всіма аспектами діяльності. Використання таких систем забезпечує ефективне управління інформацією, що є основою прийняття обґрунтованих та своєчасних рішень.

2. Процес розробки корпоративної інформаційної системи є багатогранним і включає етапи від збору вимог до проектування, реалізації та тестування. Важливою частиною є вибір технологій, що дозволяють організації ефективно вирішувати свої завдання та мінімізувати ризики, пов’язані з інформаційною безпекою та інтеграцією з іншими системами.

3. Впровадження корпоративної інформаційної системи вимагає не лише технічного забезпечення, а й організаційних змін, оскільки нові системи часто потребують адаптації існуючих бізнес-процесів. Тому важливу роль відіграють навчання персоналу, підготовка змін в організаційній структурі та взаємодії між підрозділами.

4. Теоретичні підходи до розробки включають аналіз та вибір відповідних методологій, таких як водоспадна модель, моделі гнучкого управління проектами або методи моделювання процесів. Оцінка вимог і специфікацій для майбутньої системи є основою для успішної реалізації проекту.

5. Виклики, пов'язані з впровадженням, включають управління змінами, вибір правильних інструментів для забезпечення інтеграції, а також

забезпечення високого рівня безпеки даних. Крім того, важливо враховувати потреби користувачів та забезпечити їхній комфорт при роботі з новою системою.

Загалом, теоретичні основи розробки та впровадження корпоративних інформаційних систем формують міцну базу для практичного застосування технологій у бізнесі, що дозволяє компаніям досягати високої ефективності, зменшувати ризики та забезпечувати стійкість у конкурентному середовищі.

Оцінка ризиків при впровадженні корпоративної інформаційної безпеки є невід'ємною частиною сучасного управління підприємствами, що прагнуть забезпечити стійкість своїх інформаційних систем, захист корпоративних даних і підтримання безперервності бізнес-процесів. У сучасному світі, де кіберзагрози постійно еволюціонують, ця оцінка стає критично важливою для запобігання втратам, витокам даних і порушенню довіри з боку партнерів і клієнтів.

Основні аспекти оцінки ризиків:

1. Ідентифікація загроз і вразливостей: необхідно розуміти як внутрішні (людський фактор, помилки працівників), так і зовнішні (хакерські атаки, природні катастрофи) загрози для інформаційних систем підприємства. Виявлення таких ризиків є першим кроком до їх усунення.
2. Аналіз потенційного впливу на бізнес: оцінка того, які наслідки матимуть інциденти з інформаційною безпекою для фінансових і репутаційних аспектів діяльності підприємства. Це дозволяє створити пріоритети у впровадженні заходів безпеки.
3. Впровадження політики безпеки та технічних засобів захисту: розробка чітких регламентів і процедур для збереження конфіденційності, цілісності та доступності даних є основою захисту. Технічні засоби (антивірусне ПЗ, фаєрволи, системи моніторингу) мають стати невід'ємною частиною цієї політики.
4. Навчання персоналу і підвищення обізнаності: важливо, щоб кожен співробітник розумів свою роль у забезпеченні інформаційної безпеки і мав

необхідні навички для запобігання інцидентам безпеки. Тренінги та сертифікація є важливою складовою системи захисту.

5. Моніторинг і реагування на інциденти: постійний контроль за станом безпеки дозволяє швидко виявляти та реагувати на порушення, мінімізуючи їх негативні наслідки.

6. Відповідність нормативним вимогам: дотримання стандартів і вимог законодавства (ISO/IEC 27001, GDPR) допомагає не лише захистити інформацію, а й уникнути юридичних та фінансових санкцій.

Оцінка ризиків при впровадженні корпоративної інформаційної безпеки є критично важливою для захисту підприємства від численних загроз. Це дозволяє не лише зберегти конфіденційність і цілісність даних, а й підтримувати безперервність бізнесу, зберігати репутацію та конкурентоспроможність на ринку. За допомогою систематичної оцінки ризиків та впровадження відповідних заходів безпеки організації можуть ефективно реагувати на нові виклики в сфері інформаційної безпеки, забезпечуючи стабільність і розвиток у довгостроковій перспективі.

Впровадження корпоративної інформаційної безпеки (КІБ) є критично важливим етапом для забезпечення стабільності та ефективності функціонування підприємств у сучасних умовах. Для зниження ризиків при впровадженні КІБ необхідно враховувати кілька ключових факторів:

1. Забезпечення комплексного підходу до впровадження. Це включає не лише технічну, але й організаційну підготовку, створення відповідних внутрішніх політик та процедур, що дозволяють ефективно керувати ризиками на всіх етапах проекту.

2. Оцінка та управління ризиками на кожному етапі реалізації. Систематичне оцінювання потенційних загроз та визначення заходів для їх мінімізації дозволяє знизити ймовірність негативних наслідків від впровадження КІБ.

3. Покращення навчання та підготовки персоналу. Оскільки основною проблемою для багатьох підприємств є недостатня кваліфікація

співробітників, важливо забезпечити належне навчання з питань інформаційної безпеки для всіх рівнів персоналу.

4. Адаптація до змін у технологічному середовищі. Врахування новітніх тенденцій в інформаційних технологіях і забезпечення гнучкості у системі КІБ дозволяє знижувати ризики, пов'язані з застарілими технологіями або змінами в законодавстві.

5. Моніторинг та регулярні перевірки. Постійний моніторинг ефективності системи КІБ та її адаптація до змін бізнес-процесів або зовнішніх умов є важливими інструментами для зниження ризиків і підтримки високого рівня безпеки.

Таким чином, зниження ризиків при впровадженні корпоративної інформаційної безпеки передбачає всебічний підхід, що включає технічні, організаційні та людські аспекти. Задля успішної реалізації важливо забезпечити належну координацію між усіма учасниками процесу та своєчасне реагування на зміну умов зовнішнього та внутрішнього середовища підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Є.С. Авдєєва. Методика експертної оцінки ризиків при впровадженні корпоративних інформаційних систем / Є.С. Авдєєва, В.Г. Чернов, Д.А. Градусів. - 2010. - №4. - С. 5-11.
2. Е.С. Авдєєва. Особливості впровадження КІС на підприємствах / Е.С. Авдєєва, В.Г. Чернов. // Харків. - 2010. - №7. - С. 176-177.
3. Бойчик І.М Економіка підприємства: підручник. / І.М.Бойчик. – К.: Кондор -Видавництво, 2016. – 378 с.
4. Економіка підприємства: навч. посіб. / за заг. ред. Л. С. Шевченко. – Х.: Нац. ун-т «Юрид. акад. України ім. Ярослава Мудрого», 2011. – 208 с.
5. Економіка підприємства: підруч. / За ред. С.Ф.Покропивного. - К.: КНЕУ,2006. - 528 с.
6. Економічний аналіз: Навч. посібник. За ред. Волкової Н.А./ Н.А. Волкова, Р.М. Волчек, О.М. Гайдаєнко та ін. – Одеса: ОНЕУ, ротапринт. – 2015. – 310 с.
7. Кадушіна А.І. Методика оцінки економічної ефективності IT-проектів [Електронний ресурс] / Кадушіна А.І, Михайлова Н. Б // ІФ-Консалт. - 2003. - Режим доступу до ресурсу: http://www.pmprofy.ru/content/rus/83/833-article.asp.
8. Лукін В.І. Мінімізація наслідків прояву ризиків інвестиційних проектів впровадження корпоративних інформаційних систем шляхом контролю критичних змінних [Електронний ресурс] / Лукін В.І. - 2009. - Режим доступу до ресурсу: http://www.jurnal.org/articles/2009/ekon6.html.
9. Марданов А.З. Економічні ефекти від впровадження CRM. // Корпоративний менеджмент [Електронний ресурс] / Марданов А.З. - 2009. - Режим доступу до ресурсу: http://www.cfin.ru/itm/crm/effects.shtml.
10. Миколаїв А. Оцінка ефективності від впровадження і використання методології та інструментальних засобів IBM Rational // IBM developer Works

[Електронний ресурс] / Миколаїв А. - 2009. - Режим доступу до ресурсу: http://www.ibm.com/developerworks /ru/library/r-roi/index.html.

11. Примак Т.О. Економіка підприємства: навч. посіб. / Т.О.Примак. - 4-те вид. - К.: Вікар, 2006. – 219 с.

12. ПрАТ «Тернопільський молокозавод»: офіційний сайт [Електронний ресурс]. – Режим доступу https://pjsc.molokija.com/ua/

13. Тоцький В.І. Організаційний розвиток підприємства / В.І.Тоцький, В.В.Лавриненко. - К.: КНЕУ, 2005. - 247 с.

14. Е.А.Негомедзянова. Формування моделі оцінки економічної ефективності генеруючої компанії. [Електронний ресурс] / Е.А. Негомедзянова. - 2007. - Режим доступу до ресурсу: http://www.jurnal.org/articles/2007/ekon43.html.

15. Фінансовий аналіз: навчальний посібник / І. П. Отенко, Г. Ф. Азаренков, Г. А. Іващенко. – Х.: ХНЕУ ім. С. Кузнеця, 2015. – 156 с.

16. Цілих А. Б. ТОВ КОРУС Консалтинг. Оцінка ефективності IT-проектів. Збалансований підхід. [Електронний ресурс] / Цілих А. Б. - Режим доступу до ресурсу: http://quality.eup.ru/MATERIALY5/oe-it.htm.

17. Шершньова З.Є. Стратегічне управління: підруч. /З. Є. Стратегічне управління - 2-ге вид., перер. і доп. - К.: КНЕУ, 2004. - 699 с.

18. Якимова О.Ю. Методи оцінки ефективності корпоративних інформаційних систем управління // Сучасні наукомісткі технології. [Електронний ресурс] / Якимова О.Ю. - 2006. - Режим доступу до ресурсу: www.rae.ru/snt/?section=content&op=show_article&article_id=1757.