Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет інформаційно-аналітичних технологій та менеджменту
(повна назва)

Кафедра економічної кібернетики та управління економічною безпекою
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Управління системою економічної безпеки ІТ-компанії в умовах недобросовісної конкуренції
(тема)

Виконав:
студент 2 курсу, групи УФЕБм-22-1

Забелін Є.Ю.
(прізвище, ініціали)

Спеціальність 073 Менеджмент
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління фінансово-економічною безпекою
(повна назва освітньої програми)

Керівник доц. Степаненко С. В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Полозова Т.В.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет__інформаційно-аналітичних технологій та менеджменту_____

Кафедра__економічної кібернетики та управління економічною безпекою___
(повна назва)

Рівень вищої освіти _другий (магістерський)_____

Спеціальність _073 Менеджмент_____
(код і повна назва)

Тип програми_освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління фінансово-економічною безпекою_____
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові__Забеліну Євгену Юрійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи_ Управління системою економічної безпеки ІТ-компанії в умовах недобросовісної конкуренції_____
_____
затверджена наказом по університету від 03 листопада 2023 р. № _1292 Ст_____
2. Термін подання студентом роботи до екзаменаційної комісії_____13 січня 2024 р.___
3. Вихідні дані до роботи Фінансова звітність підприємства, періодичні_____ видання, наукова література, інформаційні ресурси мережі Інтернет_____
_____
_____
_____
_____
_____
_____
4. Перелік питань, що потрібно опрацювати в роботі_____
Вступ. 1. Теоретичні аспекти управління системою економічної безпеки в умовах недобросовісної конкуренції. 2. Аналіз діяльності щодо захисту обєктів інтелектуальної власності підприємтсва ТОВ «IT-House». 3. Удосконалення системи забезпечення економічної безпеки підприємства в умовах недобросовісної конкуренції. Висновки. Перелік джерел посилання. Додаток._____
_____
_____
_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

1. Об'єкт, предмет, мета і завдання дослідження. 2. Сутність управління системою економічної безпеки. 3. Забезпечення економічної безпеки підприємства в умовах недобросовісної конкуренції. 4. Шляхи мінімізації загроз від недобросовісної конкуренції у ІТ-компаніях. 5. Тенденції розвитку ІТ-галузі. 6. Характеристика діяльності щодо захисту об'єктів інтелектуальної власності в Україні в ІТ-галузі. 7. Загальна характеристика діяльності ТОВ «IT-House». 8. Аналіз фінансово-економічного стану ТОВ «IT-House». 9. Загальні стратегії удосконалення системи забезпечення економічної безпеки. 10. Поточний стан системи забезпечення економічної безпеки підприємства «IT-House» в умовах недобросовісної конкуренції. 11. Удосконалення системи забезпечення економічної безпеки підприємства «IT-House» через стратегію розвитку персоналу за допомогою програмного забезпечення та штучного інтелекту. 12. Висновки.

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Виконання першого розділу роботи	03.11. 2023-18.11. 2023	виконано
2	Виконання другого розділу роботи	19.11. 2023-02.12. 2023	виконано
3	Виконання третього розділу роботи	03.12. 2023-19.12. 2023	виконано
4	Оформлення роботи	20.12. 2023-29.12. 2023	виконано
5	Перевірка роботи на плагіат	30.12. 2023-06.01. 2024	виконано
6	Підготовка доповіді та ілюстративного матеріалу	07.01. 2024-09.01. 2024	виконано
7	Рецензування роботи	10.01.2024-12.01. 2024	виконано
8	Подання роботи до екзаменаційної комісії	13.01.2024	виконано

Дата видачі завдання 03 листопада 2023 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Степаненко С. В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна робота: 94 с., 5 табл., 17 рис., 38 джерел, 1 додаток.

УПРАВЛІННЯ, СИСТЕМА, ЕКОНОМІЧНА БЕЗПЕКА, КОНКУРЕНЦІЯ, ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ, ПЕРСОНАЛ.

Об'єкт дослідження – система управління економічної безпеки підприємства.

Мета дослідження – аналіз теоретичних підходів та розробка практичних рекомендацій щодо удосконалення управління системою економічної безпеки підприємства в умовах недобросовісної конкуренції.

Розглянуто аспекти управління системою економічної безпеки в умовах недобросовісної конкуренції. Розкрито теоретичні засади національної системи забезпечення економічної безпеки в умовах недобросовісної конкуренції. Проаналізовано сучасні підходи шляхи мінімізації загроз від недобросовісної конкуренції у ІТ-компаніях. Проаналізовано діяльність та напрями діяльності щодо захисту об’єктів інтелектуальної власності підприємства ТОВ «IT-House». Виявлено актуальні тенденції розвитку ІТ-галузі. Визначено поточний стан системи забезпечення економічної безпеки підприємства «IT-House» в умовах недобросовісної конкуренції. Розглянуто шляхи підвищення фінансово-економічної безпеки та запропоновано перелік заходів щодо її підвищення.

ABSTRACT

Master’s thesis: 94 p., 5 tables, 17 fig., 37 sources, 1 exhibit.

ADMINISTRATION, SYSTEM, ECONOMIC SECURITY, COMPETITIVENESS, INTELLECTUAL PROPERTY, STAFF.

The object of research is the management system of economic security within the enterprise.

The purpose of the work is a theoretical approaches and development of practical recommendations for enhancing the management of the economic security system within the enterprise amidst unfair competition.

Explored aspects of managing the economic security system amidst unfair competition. Disclosed the theoretical foundations of the national system ensuring economic security amidst unfair competition. Analyzed modern approaches and strategies for minimizing threats from unfair competition in IT companies. Examined the activities and directions concerning the protection of intellectual property objects of the LLC «IT-House». Identified current trends in the IT industry's development. Determined the current state of the economic security assurance system within the «IT-House» enterprise amidst unfair competition. Explored methods to enhance financial and economic security and proposed a list of measures to improve it.

ЗМІСТ

ВСТУП

Сучасний ринок інформаційних технологій (ІТ) характеризується надзвичайною динамікою, і тут залучено велику кількість компаній, які конкурують за клієнтів, ресурси та ринкові позиції. Проте, однією з найважливіших аспектів конкурентоспроможності ІТ-компаній є їхні економічні безпека та здатність ефективно управляти несприятливими умовами ринку, зокрема умовами недобросовісної конкуренції.

Недобросовісна конкуренція, включаючи такі практики, як демпінг, крадіжка інтелектуальної власності, розповсюдження дезінформації та інші негідні способи конкуренції, може створювати серйозні загрози для стійкості та розвитку ІТ-компаній. Таким чином, питання управління системою економічної безпеки в умовах недобросовісної конкуренції стає критичним для багатьох підприємств.

Метою цієї роботи є проаналізувати сучасний стан ринку ІТ, визначити загрози, які створює недобросовісна конкуренція, та дослідити систему управління економічною безпекою ІТ-компанії в контексті недобросовісної конкуренції. Ми також розглянемо практичні кроки та стратегії, які приймаються для боротьби з цими загрозами та забезпечення стабільності та успіху компанії.

Об’єктом дослідження є управління системою фінансово-економічної безпеки підприємства.

Предметом дослідження є методи та механізми забезпечення безпеки підприємства в умовах недобросовісної конкуренції.

Задачі роботи:

– дослідити сутність визначення економічної безпеки підприємства в умовах недобросовісної конкуренції;

– виявити сучасні тенденції організаційного забезпечення економічної безпеки підприємств;

– проаналізувати діяльність підприємств ІТ-промисловості та визначити основні тенденції їх розвитку.

Дане дослідження може бути корисним як для інших ІТ-підприємств, що стикаються з подібними викликами, так і для тих, хто цікавиться питаннями управління економічною безпекою в умовах недобросовісної конкуренції.

1 ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ В УМОВАХ НЕДОБРОСОВІСНОЇ КОНКУРЕНЦІЇ

1.1 Сутність управління системою економічної безпеки

Сучасний розвиток глобальної економіки, національних фінансових систем, окремих галузей та компаній нерозривно пов'язаний не лише зі вдосконаленням технологій, появою нових методів виробництва та стратегій управління. Одним із ключових аспектів цього прогресу є забезпечення економічної стійкості суб'єктів економічних відносин на всіх рівнях, як найважливіша потреба.

Актуальність проблеми економічної безпеки визначається постійними змінами умов функціонування економічних суб'єктів, що постійно породжують нові вимоги до якісних та кількісних показників у сфері економіки. Рівень економічної безпеки безпосередньо впливає на передбачуваність можливих позитивних результатів. Отже, економічна безпека стає фундаментом для раціональної поведінки в умовах ринкових ризиків та невід'ємною умовою задоволення економічних потреб суспільства.

Поняття «економічна безпека» офіційно проголошено на сесії Генеральної Асамблеї ООН в резолюції «Міжнародна економічна безпека» та закріплено в Концепції міжнародної економічної безпеки, де зазначено, що забезпечення міжнародної економічної безпеки сприяє соціально-економічному розвитку кожної країни. Змістовне наповнення поняття «економічна безпека» випливає з розуміння економіки (грец. oikonomia – управління господарством) як найважливішої сфери суспільного буття. В такому дискурсі, основна функція безпеки зумовлена наявністю диспропорцій і дисфункцій, що виникають у процесі функціонування ринкового

економічного механізму, а також при взаємодії економічної діяльності із соціальною, екологічною та іншими сферами людської діяльності [1].

Також поняття «економічної безпеки підприємства» можна визначити як запобігання витоку конфіденційної економічної інформації з фірми, порушення комерційної таємниці, здійснення економічних диверсій.

Іноді економічну безпеку розглядають як діючу систему заходів, спрямованих на захист від недобросовісної і ненадійної співпраці, несумлінного підприємництва та недобросовісної конкуренції. Економічна безпека забезпечується узгодженою цілеспрямованою діяльністю всіх підрозділів, керівників і співробітників підприємства по виконанню спеціально розроблюваних на правовій основі інструкцій.

Деякі науковці трактують економічну безпеку підприємства як стан оптимального для підприємства рівня використання його економічного потенціалу, за якого реальні та / або можливі збитки виявляються нижчими за встановлені підприємством межі [25]. В цьому визначенні сумнівним є критерій визначення рівня безпеки – збитки. Підприємство у своїй діяльності повинно орієнтуватися на прибуток, а не збиток. І недоотримання першого також може визначатися як загроза економічному становищу, а не його безпека.

Також економічна безпека підприємства визначається як стан системи взаємодії між ним та внутрішнім/зовнішнім середовищем. Цей стан передбачає, що підприємство, спільно з державними інституціями, використовуючи свої ресурси, має здатність виявляти, уникати, нівелювати або подолати загрози, які можуть виникнути його діяльності. Економічна безпека підприємства не формується виключно його власними зусиллями, а також залежить від діяльності державних інституцій, які включають в себе правила та контроль щодо дотримання підприємствами встановлених норм [26].

Безпека підприємства включає ряд показників, таких як ефективність, стабільність, конкурентоспроможність, рентабельність, що дозволяють забезпечити працівників гідним рівнем життя. У свою чергу, забезпечення економічної безпеки передбачає такий стан економіки, при якому підтримується нормальний рівень життя населення країни і незалежність до різного роду загроз.

До об'єктів, що підлягають обов'язковій захисту від протиправних посягань, слід віднести:

– персонал підприємства, який володіє інформацією;
– фінансові ресурси;
– основний капітал;
– комерційну інформацію, бази даних, програмне забезпечення;
– засоби і системи інформатизації [2, с. 67].

Варто відзначити, що для кожного підприємства загрози, будь то внутрішнього чи зовнішнього характеру, мають свій індивідуальний характер. Заходи щодо захисту визначатимуться законодавчою базою країни, де діє підприємство, а також від оцінки кадрового потенціалу та рівня експертизи самого підприємства. До зовнішніх загроз можна віднести:

– залежність від зарубіжних ресурсів: велика залежність від імпортних ресурсів може стати вразливістю підприємства у разі геополітичних або торгових труднощів;

– залежність від імпорту продовольства і обладнання: відсутність власного виробництва та надмірна залежність від імпорту можуть призвести до збоїв у постачанні та вплинути на стабільність підприємства;

– неконкурентоспроможність підприємств: зміни на ринку, технологічний відставання та інші фактори можуть зробити підприємство неконкурентоспроможним, загрожуючи його існуванню.

– недобросовісна конкуренція: недобросовісні практики конкурентів, такі як демпінг чи крадіжка інтелектуальної власності, можуть нашкодити діяльності підприємства.

До внутрішніх загроз можна віднести дії окремих співробітників підприємства, які можуть завдати шкоди його нормальному функціонуванню, такі як розголошення комерційної таємниці, створення іміджевих проблем для підприємства за допомогою рекламних та інших нецінових методів, виникнення конфліктних ситуацій тощо.

Рівень забезпеченості економічної безпеки підприємства залежить від того, наскільки оперативно його керівництво здатне усунути можливі загрози і ліквідувати шкідливі наслідки окремих негативних складових зовнішнього і внутрішнього середовища.

Визначимо основні цілі економічної безпеки підприємства, вони представлені на рисунку 1.1.

Рисунок 1.1 – Основні цілі економічної безпеки підприємства

Проте головною метою економічної безпеки підприємства є забезпечення його стабільного та ефективного функціонування у сучасний період, а також розвиток та збереження високого потенціалу для майбутнього.

Відзначимо основні завдання економічної безпеки і підприємства:

– правовий захист підприємства, а також його показників;

– статистичний аналіз даних і прогнозування розвитку підприємства;

– правильний підбір кадрів;

– вивчення досвіду роботи інших підприємств;

– протидія комерційному шпигунству;

– виявлення і припинення протиправних дій співробітників підприємства.

Проблема забезпечення економічної безпеки підприємства виникає як у кризових періодах, так і в умовах сталого економічного розвитку. Підприємства повинні постійно дбати про підтримання нормального та максимально стабільного ритму виробництва та збуту продукції, забезпечувати фінансову стійкість та незалежність, запобігати несанкціонованому доступу до корпоративної інформації, а також боротися з недобросовісною конкуренцією. Проте, в періоди кризи особлива увага до економічної безпеки стає надзвичайно важливою, оскільки існує ризик втрати потенціалу підприємства (виробничого, науково-технічного, технологічного, кадрового тощо), який є ключовим для його функціонування.

Бізнес в Україні у високотехнологічних галузях характеризується складністю та постійною конкуренцією між підприємствами. Підприємства часто стикаються з викликами, такими як нестабільність законодавчої бази, застаріле виробниче обладнання, нестача кваліфікованої робочої сили, строга грошова та податкова політика держави, неплатоспроможність партнерів тощо. Низька завантаженість потужностей та неефективне їх використання можуть призвести до руйнування стратегічних ресурсів, які перебувають у

розпорядженні підприємства, що створює загрозу для його життєдіяльності і для суспільства, яке підприємство обслуговує.

У системі економічної безпеки підприємства виділяють об'єкти охорони, суб'єкти охорони та механізми забезпечення безпеки. Перш за все, важливо з'ясувати, що включає в себе економічний механізм безпеки підприємства. Бехтер Л. А. визначає економічний механізм безпеки підприємства як процес перетворення його зі стану загрози на стан безпеки шляхом ефективного контролю над вхідними ресурсами і виробництвом, використання внутрішніх резервів та мобілізації ресурсів, моніторингу та фільтрації потенційних загроз, їх відображення та ліквідації [24, с. 138]. По суті, визначення цього автора схоже на визначення поняття «економічна безпека підприємства», за винятком одного слова – «метод». У більшості випадків для авторів, економічна безпека визначається як «певний стан», тоді як механізм її забезпечення описує шлях до досягнення цього стану.

Наступне питання полягає в тому, яким чином механізм забезпечує досягнення бажаного стану безпеки. Відповідно до Липканя В. Л., механізм безпеки включає в себе набір цілей, функцій, принципів і методів, які взаємодіють для забезпечення ефективного функціонування системи безпеки[5]. Ладико Л. Н. визначає механізм як "порядок послідовності станів і процесів, що забезпечують економічну безпеку підприємства" [6, с. 123-124]. Ілляшенко О. В. стверджує, що механізми системи економічної безпеки підприємства визначаються як взаємодія в динаміці між елементами або підсистемами та основним суб'єктом системи, заснована на русі інформації від цих елементів або підсистем до основного об'єкта системи в протилежному напрямку [7, с. 90].

Отже, основною характеристикою економічного механізму забезпечення безпеки є «дія», тобто він не є статичним явищем, а навпаки, відповідає на запитання «як це працює?». На підставі проведених досліджень можна запропонувати власне розуміння економічного механізму забезпечення

інтелектуальної безпеки підприємства: це сукупність економічних інструментів і важелів, які впливають на систему інтелектуальної безпеки підприємства з метою досягнення бажаного стану або реакції системи безпеки. Дослідження механізму забезпечення економічної безпеки підприємства на сьогоднішній день проводиться досить активно. Коковський Л. А. пропонує наступне визначення: «сукупність методів (економічних, соціально-економічних, організаційних тощо) та інструментів (цільових програм, діагностики) для забезпечення реалізації стратегії економічної безпеки» [8]. Це визначення достатньо повно відображає основну мету механізму забезпечення безпеки.

Герасимчук З. В. та Вавадюк Н. С. визначають механізм забезпечення економічної безпеки як «послідовність дій його суб'єктів та комплекс функцій, принципів, методів та інструментів, що використовуються ними для реалізації концепції, стратегії та цільових інтегрованих програм економічної безпеки»[9]. Це визначення також враховує важливу роль методів та інструментів у забезпеченні безпеки підприємства.

Ільяшенко О. В. виділяє різні механізми економічної безпеки, але вважає, що підтримка цих механізмів – це завдання системи економічної безпеки [7]. Це дозволяє розглядати питання підтримки механізму в рамках системного підходу.

Деякі дослідники, такі як О. В. Амельницька, розглядають механізм управління економічною безпекою як невід'ємну частину системи управління підприємством і визначають його як «сукупність методів, принципів, форм, методів, важелів, заходів, пов'язаних з процесом їх взаємодії, у свою чергу, система управління – це сукупність механізмів, необхідних для реалізації цілей управління» [10]. Це підкреслює важливість включення механізму управління в загальну систему управління підприємством.

Отже, існує декілька підходів до розуміння механізму забезпечення економічної безпеки підприємства, і всі вони враховують різні аспекти його функціонування і підтримки.

З вищевикладеного видно, що дослідники мають різні підходи до того, як розуміти та визначати економічний механізм забезпечення безпеки підприємства. Однак існують загальні тенденції та спільні концепції, які представлені на рисунку 1.2.

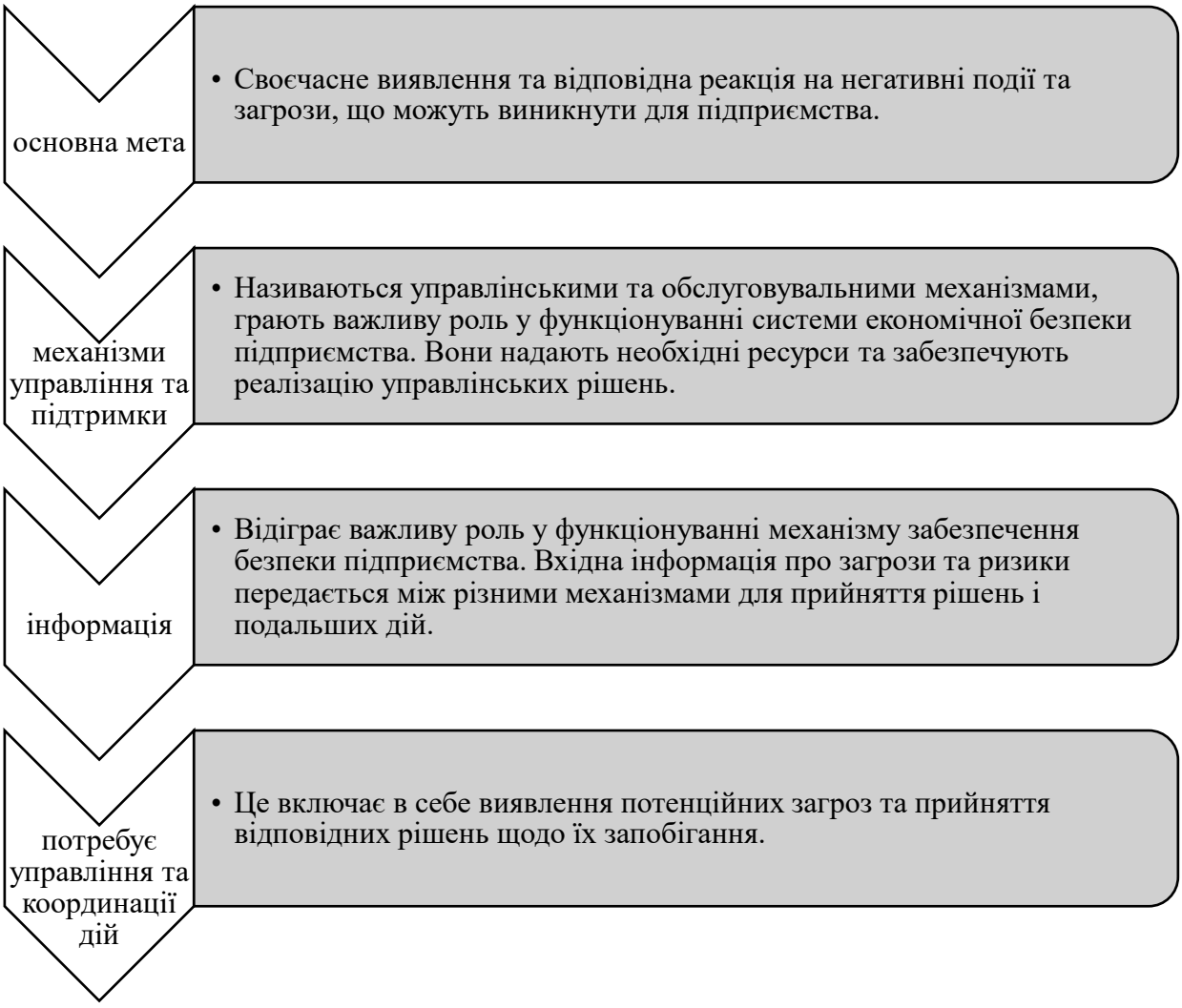

Рисунок 1.2 – Елементи механізму забезпечення економічної безпеки підприємства

Усі ці елементи спільно працюють для забезпечення економічної безпеки підприємства та зменшення ризиків. Крім того, важливим є взаємозв'язок і взаємодія між різними механізмами для досягнення бажаного рівня безпеки.

1.2 Забезпечення економічної безпеки підприємства в умовах недобросовісної конкуренції

Важливою частиною механізму ринкової економіки є конкуренція – економічний процес взаємодії та боротьби виробників за найбільш сприятливі умови для виготовлення та реалізації товарів з метою отримання найбільших прибутків. Добросовісна конкуренція сприяє розвитку та успіху компанії. Створення конкурентного середовища, захист економічної конкуренції та регулювання ринкових відносин мають прямий вплив на економічний розвиток держави. В результаті нецінової конкуренції більш успішні учасники ринку стають лідерами, що дає їм можливість розширити конкурентні інструменти: поліпшення якості продукції, розширення товарного асортименту, збільшення витрат на рекламу.

Без сумніву, конкуренція є джерелом прогресу, яке з часом призводить до значних змін і веде конкуруючі підприємства на новий етап розвитку. Проте важливо зауважити, що конкуренція не лише розкриває потенціал конкурентів, але також може породжувати жорстку боротьбу між ними, що може включати застосування жорстоких методів для досягнення переваги на ринку. У цьому контексті важливо, що кожен суб'єкт господарювання повинен розглядати конкуренцію як дієвий механізм для поліпшення своєї діяльності та забезпечення економічної безпеки.

Усі підприємства мають право на чесну конкуренцію на своїх ринках. Проте в жорсткому і не завжди справедливому світі бізнесу те, що традиційно розглядається як «справедливий», у практиці може бути несправедливим для менших учасників ринку. Засоби масової інформації часто акцентують увагу на регулюванні конкуренції між великими корпораціями, зокрема на злиттях та поглинаннях транснаціональними компаніями, що ще більше збільшують домінуючу позицію лідерів у галузі. Зазвичай такі події ретельно контролюються та перевіряються органами, що регулюють конкуренцію.

Серйозну загрозу економічній безпеці підприємства в умовах ринкової економіки, турбулентних процесів, обмеженості ресурсів або доступу до них становлять прояви недобросовісної конкуренції.

Попри те, що поняття «добросовісної конкуренції» є виключно оціночним, конкурентне право ґрунтується на презумпції визнання добросовісної поведінки підприємців, які вправі розраховувати на таку ж саму поведінку від своїх конкурентів. Натомість, вихід за межі суб'єктивного права на добросовісну конкуренцію має своїм наслідком порушення законних прав та інтересів інших суб'єктів господарювання. Будь-які дії у конкуренції, що суперечать торговим та іншим чесним звичаям у господарській діяльності, визнаються недобросовісною конкуренцією і мають своїм наслідком притягнення суб'єктів господарювання до відповідальності.

Наразі у світовій економічній практиці категорія «недобросовісна конкуренція» має досить широке тлумачення: по-перше, недобросовісну конкуренцію розглядають як проведення цілеспрямованої політики, спрямованої на усунення конкурентів із ринку; по-друге, недобросовісну конкуренцію розуміють як дії, поєднані з прямою або непрямою дезінформацією конкурентів або споживачів, введення їх в оману; по-третє, недобросовісну конкуренцію можна розглядати як будь-які дії, що полягають у використанні обманних засобів в економічному суперництві. В цілому, під

нею розуміються будь-які цілеспрямовані дії суб’єкта ринку проти конкурента, вчинені недозволеними методами [27].

Недобросовісною конкуренцією є неправомірне використання ділової репутації суб’єкта господарювання, створення перешкод суб’єктам господарювання у процесі конкуренції та досягнення неправомірних переваг у конкуренції, неправомірне збирання, розголошення та використання комерційної таємниці [28].

Національна система забезпечення економічної безпеки в умовах недобросовісної конкуренції – це комплекс заходів та політичних стратегій, розроблений національними урядовими інстанціями, з метою забезпечення стійкості і конкурентоздатності національної економіки в умовах негідної або недобросовісної конкуренції. Ця система орієнтована на захист законних інтересів суб'єктів господарювання, сприяння чесним конкурентним умовам на ринку, та запобігання шкідливим практикам, що можуть порушити економічну стабільність країни.

Дослідження показують, що малі підприємства також часто стикаються з недобросовісною конкуренцією, і це відбувається набагато частіше, ніж може здатися. Майже чверть малих та середніх підприємств (МСП) у Великобританії вважають, що їм завдається шкоди через несправедливі практики, такі як узгоджені ціни та домовленості щодо тендерних пропозицій [3], за інформацією Управління добросовісної торгівлі. Крім того, кожне третє МСП стверджує, що вони мають інформацію про антиконкурентну діяльність у своїх галузях, і кожна п'ята компанія (22 %) відчуває себе жертвою антиконкурентної поведінки.

Управління добросовісної торгівлі Великобританії закликає МСП визнати антиконкурентну практику на своїх ринках та спільно з ними вживати заходів проти компаній, які порушують законодавство про конкуренцію.

Незважаючи на очевидну високу обізнаність щодо антиконкурентної поведінки, лише меншість опитаних МСП заявили, що вони повідомлять про це державним регуляторам:

– лише 22 % повідомили б про встановлення ціни угоди між конкурентами;

– лише 9 % повідомили б про те, що більший конкурент намагається витіснити їх з ринку, знизивши його ціни нижче собівартості.

Дослідження Управління добросовісної торгівлі показують, що багато малих та середніх підприємств можуть втратити переваги чесних та конкурентних ринків. Опитування також показує, що більше половини підприємств вважають, що галузь, в якій вони працюють, може підвищити свою конкурентоспроможність. Більше третини МСП вважають, що нові компанії мають труднощі з виходом на ринки, і 16 % заявляють, що не можуть вільно і чесно конкурувати за нові контракти, і цей показник ще більший для деяких галузей, наприклад, будівництва – 21 % [3].

Управління конкурентною політикою в Україні потребує розвитку додаткових механізмів, щоб забезпечити рівний доступ до ресурсів і можливість використання найбільш ефективних бізнес-технологій.

Елементи національної системи забезпечення економічної безпеки в умовах недобросовісної конкуренції представлені на рисунку 1.3.

Ця система сприяє створенню чесних та рівних умов для всіх суб'єктів господарювання, підтримує економічну стійкість країни та сприяє розвитку конкурентоспроможності національної економіки.

Закон України "Про захист від недобросовісної конкуренції" розглядає три основні варіанти недобросовісної конкуренції: незаконне використання репутації суб'єкта господарювання, створення завад для інших суб'єктів господарювання у конкурентному процесі та досягнення недобросовісних переваг у конкурентній боротьбі, а також незаконне збирання, розкриття та використання комерційної таємниці [11].

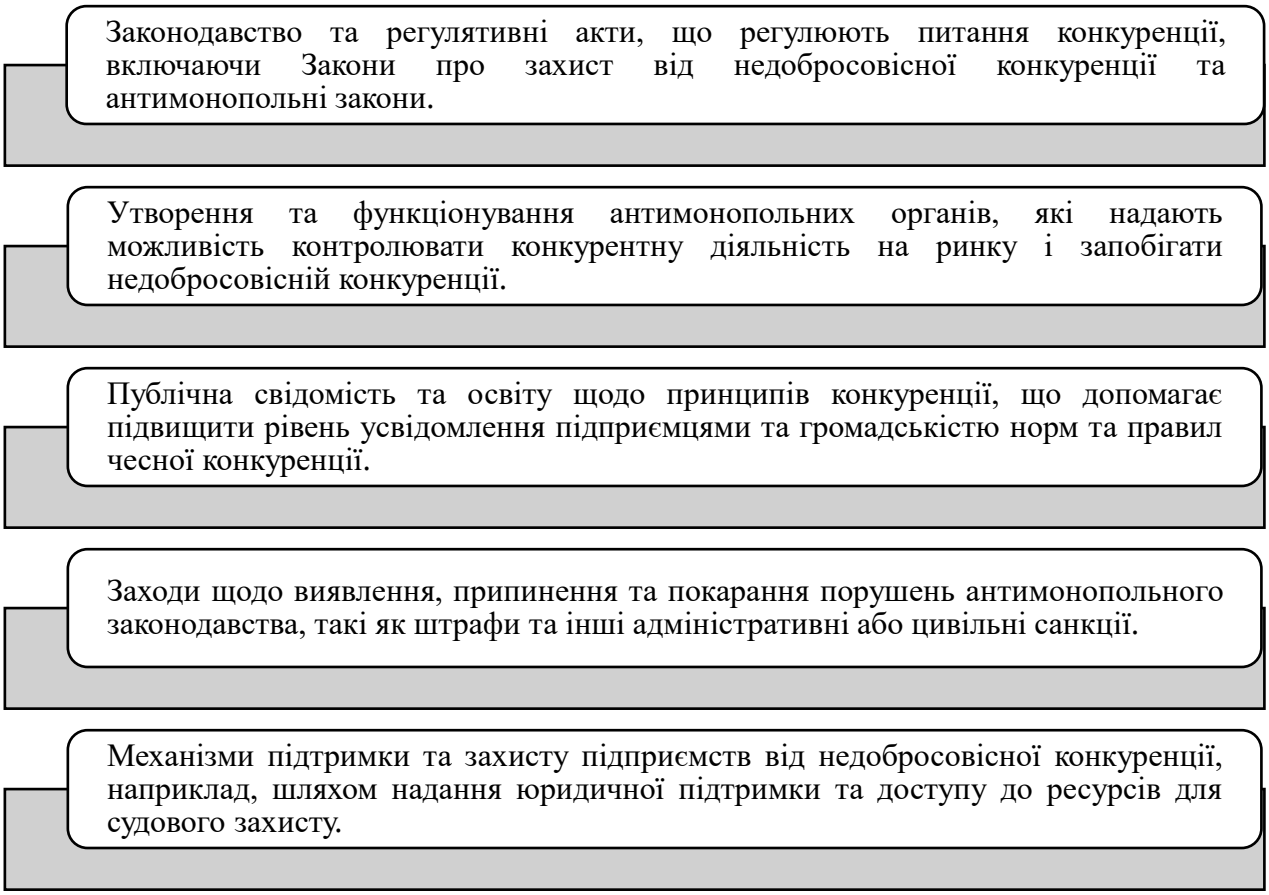

Рисунок 1.3 – Елементи національної системи забезпечення економічної безпеки

Кожен з цих видів може бути розглянутий як потенційна загроза для економічної безпеки підприємства, і розгляньмо їх докладніше.

Перший вид – це незаконне використання репутації суб'єкта господарювання. Згідно зі статтею 2 Закону України «Про ринки капіталу та організовані товарні ринки», ділова репутація – це інформація, яка документально підтверджує роботу фізичної або юридичної особи і дозволяє зробити висновок щодо її відповідності вимогам законодавства, бізнес-практики і професійної етики, а також містить інформацію про щестомірність, професійні та управлінські навички фізичної особи [12]. В Законі про захист від недобросовісної конкуренції наведено різні методи незаконного використання репутації, такі як незаконне використання торгових марок, продуктів інших виробників, копіювання зовнішнього вигляду виробу та

порівняльна реклама. З нашого погляду, це досить обмежений підхід, оскільки він обмежується лише на продукції або послугах суб'єкта, і дає оцінку самому об'єкту, а не суб'єкту. Ми вважаємо, що до цього виду недобросовісної конкуренції також варто включити дискредитацію суб'єкта господарювання, яка в законі пов'язана з другим видом недобросовісної конкуренції. Дискредитація суб'єкта господарювання описується як поширення будь-якої форми неправдивої, неточної або неповної інформації, пов'язаної з особою або діяльністю суб'єкта господарювання, включаючи інформацію про його товари, яка може завдати шкоди репутації суб'єкта господарювання [11].

Другий вид недобросовісної конкуренції, згідно з законом, включає створення завад іншим суб'єктам господарювання у конкурентному процесі та досягнення недобросовісних переваг у конкурентній боротьбі. Основні методи включають дискредитацію суб'єкта господарювання, спрямування суб'єкта господарювання до бойкоту, спрямування постачальника до дискримінації покупця, підкуп працівника постачальника, підкуп працівника покупця, досягнення недобросовісних переваг у конкурентній боротьбі та поширення недостовірної інформації [11].

Третій вид недобросовісної конкуренції включає незаконне збирання, використання та розголошення комерційної таємниці. Законом визначено різні методи незаконного збирання, розголошення та використання комерційної таємниці. Згідно з Цивільним кодексом України, комерційна таємниця – це інформація, яка є секретною і недоступною для осіб, які мають справу з такою інформацією, та має комерційну цінність. Комерційною таємницею можуть бути технічні, організаційні, комерційні та іншого виду дані, за винятком тих, які за законом не вважаються комерційною таємницею [13].

Застосування будь-яких із цих методів до суб'єкта господарювання суттєво впливає на його безпеку.

Напрями для вдосконалення системи захисту інтересів компаній від недобросовісної конкуренції в Україні представлені на рисунку 1.4.

Загалом для ефективного захисту інтересів суб’єкта необхідно не тільки боротися з недобросовісною конкуренцією, використовуючи нормативні та адміністративні методи, а й створювати такі умови, за яких було б невигідно порушувати правила добросовісної конкуренції [29].

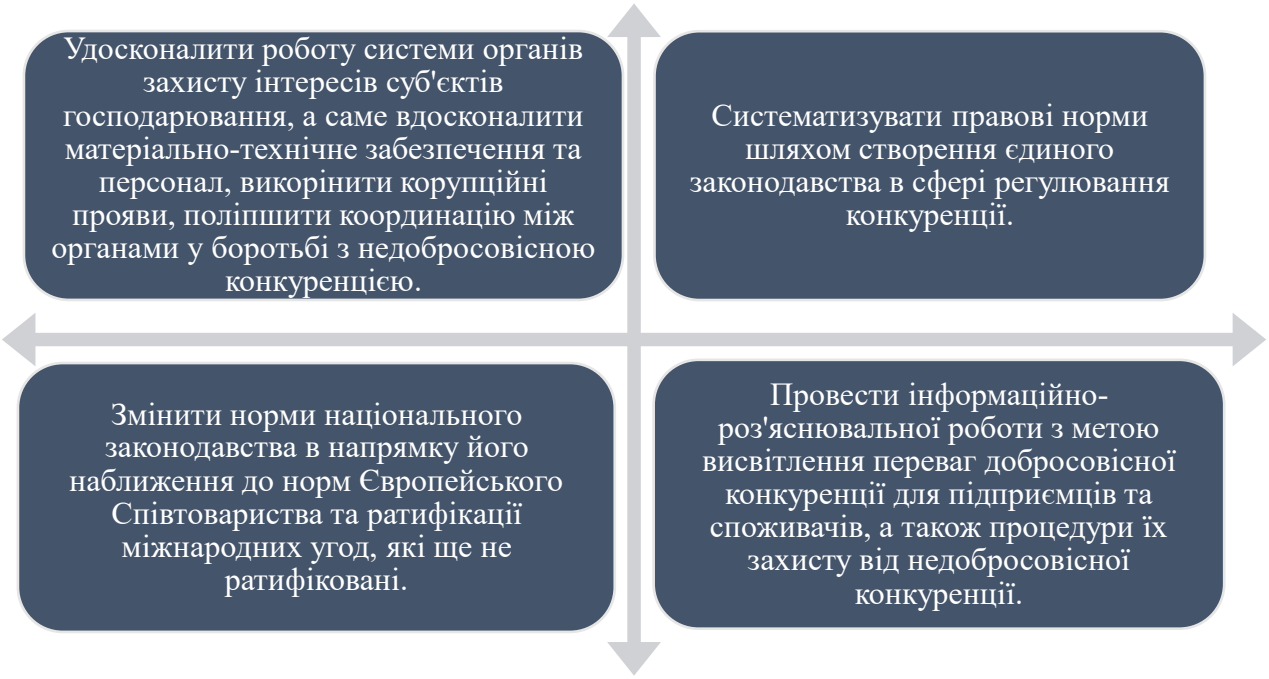

Рисунок 1.4 – Напрями вдосконалення системи захисту інтересів компаній від недобросовісної конкуренції в Україні

1.3 Шляхи мінімізації загроз від недобросовісної конкуренції у IT-компаніях

У сфері бізнесу існує безліч ризиків та небезпек. Деякі з них можуть призвести до краху підприємства, тоді як інші можуть значно пошкодити його фінансово чи репутаційно. Вирішення таких проблем може вимагати значних зусиль і коштів. Незважаючи на це, керівники та експерти з управління

ризиками мають можливість передбачати та готуватися до таких сценаріїв, незалежно від масштабу підприємства.

Все, що загрожує можливості компанії досягти своєї мети або досягти своїх фінансових цілей, називається бізнес-ризиком. Ці ризики походять з різних джерел, тому не завжди винен керівник компанії чи менеджер. Натомість ризики можуть надходити з інших джерел фірми або можуть бути зовнішніми – від законодавства до загальної економіки.

Ризики за походженням можна розділити на зовнішні та внутрішні. Внутрішні ризики виникають в межах самої компанії під час звичайних операцій. Ці ризики можна передбачити з певною достовірністю, що дає компанії можливість знизити їх вплив.

Внутрішні фактори ризику поділяються на людські, технологічні та фізичні. Людський фактор ризику включає страйки, нечесність працівників, проблеми з управлінням та інші аспекти. Технологічний ризик полягає в непередбачених змінах у виробництві чи постачанні товарів чи послуг. Фізичний ризик – це втрата чи пошкодження активів компанії. Для зменшення внутрішніх ризиків компанії можуть використовувати різні методи, такі як страхування, щоб захистити себе від можливих втрат. Оскільки зовнішні ризики неможливо передбачити з точністю, компанії важко знизити їх вплив.

Структура зовнішніх та внутрішніх ризиків наведена на рисунку 1.5.

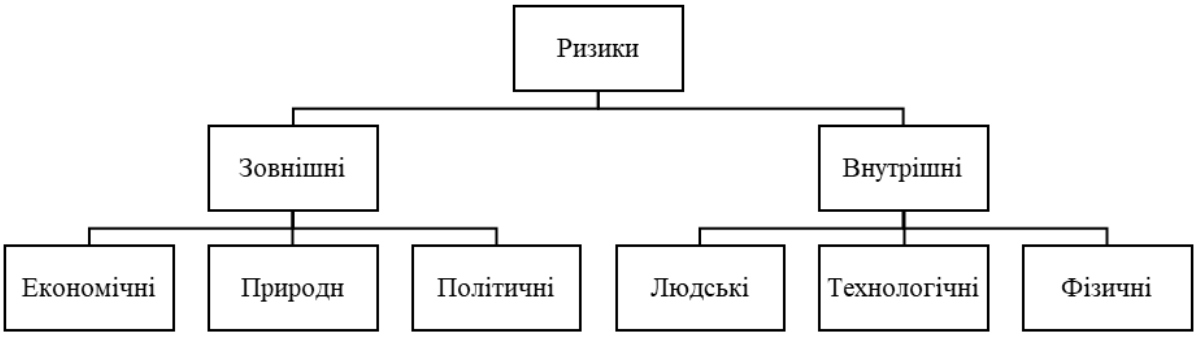

Рисунок 1.5 – Структура зовнішніх та внутрішніх ризиків

Ризик завжди пов’язаний із поняттям безпеки. Забезпечення безпеки підприємства є одним з головних завдань менеджменту.

Серйозну загрозу економічній безпеці підприємства в умовах ринкової економіки, турбулентних процесів, обмеженості ресурсів або доступу до них становлять прояви недобросовісної конкуренції.

В Законі України «Про захист від недобросовісної конкуренції» визначено три форми недобросовісної конкуренції: неправомірне використання ділової репутації суб’єкта господарювання, створення перешкод суб’єктам господарювання в процесі конкуренції та досягнення неправомірних переваг у конкуренції, неправомірне збирання, розголошення та використання комерційної таємниці [30].

Кожна з цих форм може бути ідентифікована як внутрішня чи зовнішня загроза економічній безпеці підприємства. Розглянемо детальніше кожну з форм.

Перша форма – неправомірне використання ділової репутації суб’єкта господарювання. Відповідно до ст. 2 Закону України «Про ринки капіталу та організовані товарні ринки» Ділова репутація – сукупність документально підтвердженої інформації про фізичну або юридичну особу, що дає можливість зробити висновок про відповідність її діяльності вимогам законодавства, діловій практиці та професійній етиці, а також відомості про порядність, професійні та управлінські здібності фізичної особи [31]. Ділову репутацію прийнято розглядати як результат сприйняття діяльності її власника оточуючими. В Законі України «Про захист від недобросовісної конкуренції» до основних методів неправомірного використання ділової репутації відносять неправомірне використання позначень, неправомірне використання товару іншого виробника, копіювання зовнішнього виду виробу, порівняльну рекламу [3]. З нашої точки зору, це дещо звужений підхід. В такому випадку мова лише про одну складову діяльності юридичної чи фізичної особи – її продукцію, послуги тощо, скоріше про репутацію продукції, дається оцінка не

суб’єкту, а об’єкту. До цієї форми, на нашу думку, необхідно було б віднести дискредитацію суб’єкта господарювання, яка в законі пов’язана з другою формою недобросовісної конкуренції. «Дискредитацією суб'єкта господарювання є поширення у будь-якій формі неправдивих, неточних або неповних відомостей, пов'язаних з особою чи діяльністю суб'єкта господарювання, у тому числі щодо його товарів, які завдали або могли завдати шкоди діловій репутації суб'єкта господарювання» [30].

Другою формою в законі зазначено створення перешкод суб’єктам господарювання в процесі конкуренції та досягнення неправомірних переваг у конкуренції. Основними методами визначені: дискредитація суб’єкта господарювання; схилення суб’єкта господарювання до бойкоту; схилення постачальника до дискримінації покупця; підкуп працівника постачальника; підкуп працівника покупця; досягнення неправомірних переваг у конкуренції; поширенням інформації, що вводить в оману [30].

Третьою формою недобросовісної конкуренції є неправомірне збирання, використання та розголошення комерційної таємниці. Основними методами в законі визначено неправомірне збирання, розголошення схилення до розголошення комерційної таємниці, неправомірне використання комерційної таємниці [30]. Згідно ЦКУ ст.505 «комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці [32].

Застосування всіх цих методів до суб’єкта господарювання значною мірою відображається на рівні його безпеки.

В умовах швидкого розвитку інформаційних технологій та постійних змін на ринку виникає безліч викликів для ІТ-компаній. Саме одним із найбільших викликів є недобросовісна конкуренція, яка може підірвати економічну стійкість компанії. Організація системи економічної безпеки стає надзвичайно важливою для захисту інтересів ІТ-підприємств [38].

Перший і найбільш очевидний крок для забезпечення економічної безпеки ІТ-компанії – це правовий захист її інтелектуальної власності. Інновації та розробки є основною цінністю для багатьох ІТ-підприємств, тому важливо ретельно захищати свої інтелектуальні права. Деякі ключові кроки в цьому напрямку включають:

– реєстрація авторських прав, патентів та товарних знаків: важливо зареєструвати всі інтелектуальні права на продукти і технології. Це надає юридичну підтримку у разі порушення цих прав і дозволяє пред'явити вимоги до порушників;

– політика конфіденційності: складання і впровадження політики конфіденційності для компанії. Ця політика повинна визначати, які інформаційні ресурси вважаються конфіденційними, та обмежувати доступ до них;

– судові позови: якщо інтелектуальна власність була порушена, треба подавати судові позови проти порушників. Захист інтелектуальної власності в судах може допомогти відновити збитки та запобігти подібним порушенням у майбутньому [14].

Важливо не тільки захищати інтелектуальну власність від зовнішніх загроз, але й контролювати та моніторити внутрішню безпеку компанії. Внутрішні порушення та несанкціонований доступ до конфіденційної інформації можуть бути також значущими загрозами. Основні кроки в цьому напрямку включають:

– система моніторингу доступу: встановлення системи моніторингу, яка відстежує доступ до важливих даних і ресурсів. Ця система може автоматично реєструвати і аналізувати всі спроби доступу до конфіденційної інформації;

– регулярна перевірка на внутрішні порушення: Проведення регулярних перевірок, спрямоване на виявлення внутрішніх порушень та несанкціонованого доступу до конфіденційної інформації.

Спроможність реагувати на порушення безпеки важлива для забезпечення економічної безпеки компанії. Якщо порушення сталося, критично мати чіткий план дій, який дозволяє відповісти на нього ефективно. Основні кроки в цьому напрямку включають:

– план дій при виявленні порушень безпеки: розроблення плану дій, який визначає кроки, які необхідно вжити при виявленні порушення безпеки. Цей план повинен охоплювати всі можливі сценарії, включаючи інциденти з кібербезпеки;

– навчання співробітників: проведення навчання та тренінгів для співробітників, щоб вони знали, як реагувати на інциденти безпеки та сприяли зменшенню ризику.

Співпраця з правоохоронними органами та кіберполіцією може бути дуже корисною для виявлення та переслідування порушників. Деякі ключові кроки в цьому напрямку включають:

– співпраця з органами правопорядку: співпрацювання з органами правопорядку, надавання їм інформації про порушення безпеки;

– оновлення списку контактів: постійне оновлення списку контактів для швидкого реагування на надзвичайні ситуації. Швидкий зв'язок з правоохоронними органами може допомогти розслідувати порушення ефективно.

Кризова комунікація є важливим аспектом забезпечення економічної безпеки в умовах недобросовісної конкуренції. Якщо сталася подія, яка може негативно вплинути на репутацію компанії, ефективна комунікація допоможе зменшити можливі збитки. Кроки в цьому напрямку включають:

– план комунікації: розробка плану комунікації для взаємодії з клієнтами, контрагентами та громадськістю у разі кризової ситуації. Цей план повинен визначати комунікаційні канали та відповідальних за них осіб;

– висвітлення інцидентів: висвітлювання інциденти та заходів, які приймаються для їх вирішення. Транспарентність і відкритість в комунікації можуть допомогти заспокоїти стейкхолдерів та зберегти довіру.

Умови на ринку та загрози постійно змінюються, тому важливо проводити постійну оцінку ризиків та адаптувати ваші стратегії. Основні кроки в цьому напрямку включають:

– регулярні аудити безпеки: проведення регулярних аудитів безпеки, щоб визначити можливі ризики та вразливості. Аудити допоможуть виявити проблеми та вжити заходи для їх вирішення;

– зміна стратегій і політик: зміна стратегії і політики відповідно до нових загроз і відповідей на них. Адаптування стратегій відповідно до змін на ринку [15].

Кібербезпека важлива для забезпечення економічної безпеки ІТ-компаній. Наймання та тренування фахівців у сфері кібербезпеки важливо для захисту мережі та даних компанії від кібератак. Основні кроки в цьому напрямку включають:

– пошук кваліфікованих фахівців: проведення пошуку та наймання кваліфікованих фахівців з кібербезпеки. Вони повинні мати необхідні навички та досвід для виявлення та захисту від кіберзагроз;

– тренування персоналу: навчання персоналу компанії основам кібербезпеки. Інформовані співробітники можуть допомогти запобігти багатьом кіберзагрозам та виявити їх раніше [16].

Управління репутацією є важливим аспектом забезпечення економічної безпеки в умовах недобросовісної конкуренції. Репутація компанії може визначити її успіх на ринку. Деякі ключові кроки в цьому напрямку включають:

– імідж компанії: активна взаємодія з клієнтами та стейкхолдерами, демонстрування зобов'язанності до якості та безпеки;

– кризовий PR: розроблення плану кризового PR, який дозволить реагувати на інциденти та ефективно керувати інформаційними потоками під час кризових ситуацій.

Умови недобросовісної конкуренції вимагають від IT-компаній комплексного підходу до забезпечення економічної безпеки. Інтелектуальна безпека виступає як важливий елемент системи забезпечення безпеки підприємства. Захист інтелектуальної власності, розвиток інновацій, співпраця з правоохоронними органами та кіберполіцією, ефективна кризова комунікація, постійна оцінка ризиків та залучення фахівців у сфері кібербезпеки є важливими стратегічними напрямками для забезпечення економічної безпеки компанії в умовах недобросовісної конкуренції. Розробка та впровадження цих стратегій допоможуть зменшити ризики та зберегти стабільність та успіх підприємства на ринку.

Висновки до першого розділу

В першому розділі роботи проведене теоретичне дослідження аспектів управління системою економічної безпеки в умовах недобросовісної конкуренції. Розглянута сутність управління системою економічної безпеки, основні цілі економічної безпеки підприємства та були визначені основні елементи механізму забезпечення економічної безпеки підприємства.

Проаналізовано забезпечення економічної безпеки в умовах недобросовісної конкуренції. Розглянуто поняття «недобросовісна конкуренція». Також були виявлені елементи національної системи забезпечення економічної безпеки та основні напрями вдосконалення системи захисту інтересів компаній від недобросовісної конкуренції в Україні.

Огляд структури зовнішніх та внутрішніх ризиків показав, що загалом ризиків для компанії багато. Також було виділено три форми недобросовісної конкуренції та основні кроки для забезпечення економічної безпеки ІТ-компанії.

2 АНАЛІЗ ДІЯЛЬНОСТІ ЩОДО ЗАХИСТУ ОБ'ЄКТІВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В УКРАЇНІ ТА ПІДПРИЄМТСВА ТОВ «IT-HOUSE»

2.1 Тенденції розвитку IT-галузі

На сьогоднішній день українська галузь інформаційних технологій займає провідні позиції у світі. Незважаючи на те, що протягом останніх кількох років ринок IT-послуг переживає скрутні часи через світову кризу, спричинену пандемією COVID-19 та повномасштабною війною, галузь є дуже важливою. Зростання IT-ринку України в пропорції до 50 % тривало до самої війни, у галузі було зайнято приблизно 275 тисяч осіб. У лютому 2022 року, за даними Національного банку України, показник експорту українського IT-ринку досяг 839 млн доларів. Український IT-ринок у воєнний період забезпечував 37 % експорту послуг в сфері комп'ютерних послуг, що становило 7,3 млрд доларів надходжень [17]. Зараз Україна та IT-галузь, зокрема, стикаються з викликами війни. Це стосується збереження та балансування людського капіталу, можливості для подальшого сталого зростання. Конкуренція на ринку фахівців встановлюватиме нові планки щодо кваліфікації, знань та навичок, що мають стратегічне значення для IT-галузі. У таких умовах аналіз динаміки розвитку та подальші перспективи IT-галузі в Україні, а також її вплив на глобальну економіку робить обрану тему дослідження актуальною.

Упродовж останніх років український ринок інформаційних технологій проявляв стабільний зріст на рівні 20-30 % щорічно. Важливо відзначити, що показник доходу збільшувався в 4-5 разів швидше, ніж в середньому у всьому світі, що робить український IT-сектор дуже привабливим для інвестицій [18]. Українські компанії щорічно укладають угоди на суму від 300 до 700 млн доларів США [17].

За результатами 2021 року, обсяг IT-послуг становив 87,95 мільярда гривень, що на 23,32 % більше, ніж у 2020 році. Найбільшу частину IT-послуг використовують підприємства та установи, які становлять в середньому від 93 % до 96 % ринку, тоді як населення використовує приблизно 1-3 %, і інші категорії споживачів – 1-4 %.

Відповідно до даних Нацбанку, обсяг IT-експорту з України зменшився на 2,4 % у порівнянні з минулим півріччям, але збільшився на 3,1 %, якщо порівнювати з минулорічними показниками. У липні 2023-го виторг становив $559 млн, це на $17 млн більше, аніж у липні 2022 року.

Показник за червень цього року становив $573 млн. Загалом же після початку повномасштабної війни обсяг IT-експорту за місяць тримається на рівні $500–600 млн із незначними коливаннями. У липні 2022-го цей показник становив $542 млн, у липні 2021-го — $574 млн, а от у червні 2020-го – $413 млн [33].

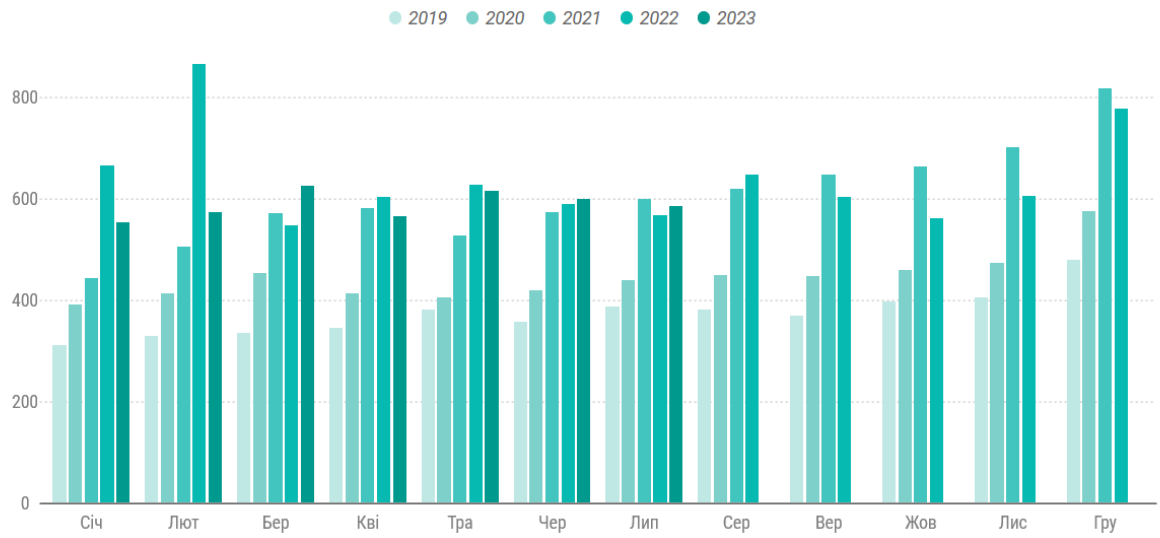

Рисунок 2.1 – Обсяг IT-ринку України, млн доларів [33]

Більшість українських IT-компаній спеціалізується на наданні послуг іноземним замовникам у сфері розробки програмного забезпечення та сервісів.

Основною діяльністю аутсорсингових ІТ-компаній є виконання розробки програмних продуктів за замовленням інших інтермедіарів в ІТ-галузі, які, у свою чергу, надають такі послуги своїм власним клієнтам. Щодо двох інших сегментів – розробка готового програмного забезпечення та створення апаратного забезпечення, то вони менше розвинуті [19].

Згідно з даними Національного Банку України протягом 2022 року український ІТ-сектор збільшив експорт на 400 мільйонів доларів, що становить зростання на 5,8 % порівняно з 2021 роком, і загальна сума експорту становить 7,34 млрд доларів. ІТ-сектор став найбільшим внеском у загальний експорт послуг. Працівники ІТ-сектору демонстрували швидку адаптацію до перешкод, таких як відключення електроенергії під час російських обстрілів. Навіть у листопаді-грудні експорт комп'ютерних послуг з України зростав навіть при максимальній інтенсивності обстрілів та відключеннях електропостачання. У грудні експорт склав 751 млн доларів, що більше, ніж будь-коли раніше, окрім лютого 2022 року. Експортні доходи співвідносяться з кількістю контрактів, укладених замовниками сервісних ІТ-компаній. Укладання нових угод стає викликом для українських компаній у нинішній ситуації. Експерти прогнозують, що до кінця війни суттєвого зростання та нових замовлень не передбачається [20].

Агресивне повномасштабне вторгнення рф зупинило невпинний ріст експорту ІТ-послуг. Апогею даний показник ІТ-активності досягнув напередодні російського вторгнення у 4 кварталі 2021 року, коли в країну було заведено 2.1 млрд доларів США. З тих пір середні обсяги експорту комп'ютерних послуг поступово спустилися до відмітки 1.7 млрд доларів, тобто рівень просадки обсягів квартальної експортної ІТ-виручки склав близько -20 %.

Частка сектору в загальному експорті товарів та послуг України за півтора роки війни зросла з 8.8 % до 13.4 %, наразі розгляд ІТ-сектору в якості локомотива нарощення експортних потужностей далекий від довоєнних

оптимістичних очікувань [35]. Ця статистика у графічному вигляді представлена на рисунку 2.2.

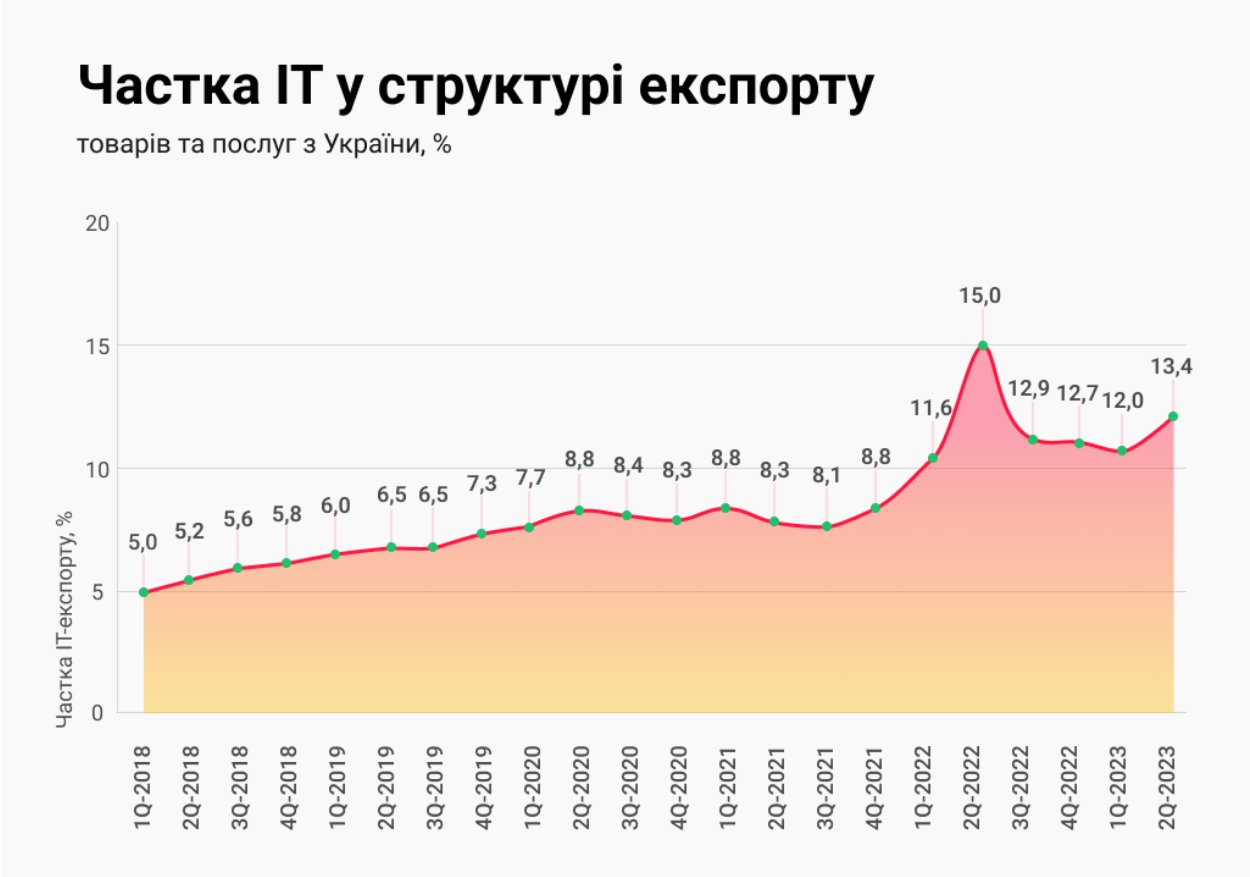

Рисунок 2.2 – Частка IT-сектору у структурі експорту [35]

Під час першого року війни найбільш швидкими темпами кількість активних IT-ФОПів зростала в Волинській, Хмельницькій, Кіровоградській, Полтавській, Чернівецькій та Івано-Франківській областях. Високий приріст індивідуальних айті-бізнесменів на рівні 17-20 % спостерігався в західних і центральних регіонах, котрі відносно менше постраждали від агресивних дій ворога [35]. Приріст кількості IT-ФОП в перший рік війни представлено на рисунку 2.3.

Рисунок 2.3 – Приріст кількості ІТ-ФОП в перший рік війни [35]

Українське ІТ постраждало двічі. Від початку війни кількість вакансій скоротилася не лише через військові дії і проблеми в українських замовників, але й через загальносвітову кризу. Статистика зміни загальної кількості вакансій відображена на рисунку 2.4. Якщо спочатку ринок втрачав більшість замовлень через цілковиту невизначеність і зарубіжні клієнти розривали контракти, бо ризики співпрацювати з фахівцями країни у стані війни були

захмарними, то восени до негативних трендів додалися блекаути. Ніхто не міг передбачити, коли та наскільки відключать світло, і не кожен замовник міг із розумінням поставитися до ситуації [34].

Рисунок 2.4 – Статистика зміни загальної кількості вакансій в Україні в ІТ-галузі [34]

Таким чином, за номінальним зростанням окремих індикаторів ІТ-сектору, в тому числі офіційної кількості ФОП чи гривневої виручки, можуть бути приховані достатньо невтішні тенденції руйнівного впливу воєнно-політичних та макроекономічних факторів на галузь, котра традиційно вважалася драйвером майбутнього успіху української економіки.

2.2 Характеристика діяльності щодо захисту об'єктів інтелектуальної власності в Україні в ІТ-галузі

В Україні захист об'єктів інтелектуальної власності в ІТ-галузі регулюється законодавством, яке включає в себе різноманітні аспекти захисту.

Авторське право – застосовується до програмного забезпечення, баз даних, веб-сайтів тощо. Авторське право виникає автоматично з моменту

створення твору. За останні роки в Україні зросла кількість зареєстрованих авторських прав на програмне забезпечення та інші ІТ-продукти. Згідно з Державним агентством із захисту інтелектуальної власності (ДАЗВ), кількість поданих заявок на реєстрацію авторських прав у галузі ІТ продовжує зростати.

Патентування – у разі новаторських технологій, винаходів або відкриттів, компанії можуть подавати заявки на отримання патентів, що надає їм ексклюзивні права на використання винаходу протягом певного періоду. Кількість поданих заявок на отримання патентів в ІТ-галузі в Україні також збільшується. Це свідчить про активний розвиток новаторських технологій та інновацій в цій сфері.

Товарні знаки – захист товарних знаків дозволяє компаніям визначати свої продукти чи послуги та захищати їх від використання конкурентами. Україна реєструє значну кількість товарних знаків в ІТ-секторі. Це важливо для захисту брендів та ідентифікації продуктів чи послуг на ринку.

Комерційна таємниця – іноді інформація, яка не є відомою загальному публічному доступу, може бути захищена як комерційна таємниця, наприклад, секрети розробки ПЗ, алгоритми тощо. Інформація про захист комерційної таємниці у сфері ІТ часто не є публічною. Проте, компанії активно застосовують заходи щодо збереження конфіденційної інформації, використовуючи нерозголошені алгоритми, технологічні рішення та інші методи захисту.

Державне підприємство «Український інститут інтелектуальної власності» (Укрпатент) виконує функції, покладені на нього Міністерством розвитку економіки, торгівлі і сільського господарства України. Вони є Уповноваженим органом управління, що надає послуги з проведення експертизи заявок на об'єкти промислової власності, готує відомості для державної реєстрації охоронних документів та здійснює технічне адміністрування державних реєстрів.

У своїй діяльності Укрпатент керується рядом законів України, серед яких «Про охорону прав на винаходи і корисні моделі», «Про охорону прав на промислові зразки», «Про охорону прав на компонування напівпровідникових виробів», «Про охорону прав на знаки для товарів і послуг», а також «Про правову охорону географічних зазначень». Виконання цих законів дозволяє регулювати та забезпечувати захист прав на інтелектуальну власність в різних сферах та виданнях.

Так наприклад виглядала динаміка надходження заявок через систему електронного подання у 2021 (рис. 2.5) [36].

Рисунок 2.5 – Динаміка надходження заявок через систему електронного подання у 2021 році [36]

У 2022 році Укрпатент отримав 57,300 заявок на об’єкти промислової власності. Це включало близько 3,9 тисяч заявок на винаходи, 8,5 тисяч – на корисні моделі, 2,7 тисячі – на промислові зразки і майже 42,2 тисячі – на знаки для товарів і послуг.

З використанням системи електронного подання заявок у 2022 році було подано 14,998 заявок на об’єкти промислової власності. З них 939 (6,3 %)

стосувалися винаходів, 722 (4,8 %) – корисних моделей, 771 (5,1 %) – промислових зразків і 12,566 (83,8 %) – знаків для товарів і послуг.

Виходячи з приведених статистичних даних з'ясовано, що в Україні ведеться активна робота з убезпечення об'єктів інтелектуальної власності.

Також згідно Звіту Антимонопольного комітету України за 2022 рік, затвердженого розпорядженням АМКУ від 12.03.2023 р. №1-рп, органами Антимонопольного комітету України було припинено 168 порушень Закону України «Про захист від недобросовісної конкуренції». Із них – 40 порушень у вигляді недобросовісної конкуренції, стосовно яких Комітетом було прийнято рішення про накладення штрафних санкцій та 128 дій, що містили ознаки таких порушень, які було припинено відповідно до наданих органами Комітету рекомендацій суб'єктам [37]. Статистичні дані згідно звіту АМКУ за 2022 рік приведено на рисунку 2.6.

Очевидним є, що значна кількість дій, які характеризуються як недобросовісна конкуренція, пов'язані з порушення прав на об'єкти інтелектуальної власності, таких як: знаки для товарів і послуг (торговельні марки), корисні моделі, винаходи, промислові зразки тощо.

Таким чином, захист об'єктів прав інтелектуальної власності шляхом звернення з відповідною заявою про порушення прав від недобросовісної конкуренції до органів Антимонопольного комітету України (АКМ) є лише одним з варіантів захисту. Однак на сьогоднішній день, така стратегія в повній мірі не захистить права інтелектуальної власності, та не приведе до конкретного результату, а може слугувати виключно додатковим елементом у подальшому судовому захисті. Висновки (рішення) органів АКМ на користь заявника можуть слугувати додатковими доказами при вирішенні конкретного спору між суб'єктами господарювання.

Захист інтелектуальної власності в ІТ-галузі є важливою складовою для стимулювання інновацій та розвитку технологій. Компанії часто вживають заходів для захисту своїх інтелектуальних прав, будучи уважними до

патентної чи авторської належності, підписуючи відповідні угоди та використовуючи захисні стратегії.

Рисунок 2.6 – Статистичні дані згідно звіту Антимонопольного комітету України за 2022 рік [37]

Тому аналіз діяльності щодо захисту об’єктів інтелектуальної власності підприємства та шляхи мінімізації загроз від недобросовісної конкуренції у ІТ-компаніях дуже важливі у наш час.

2.3 Загальна характеристика діяльності ТОВ «IT-House»

Товариство з обмеженою відповідальністю «IT-House» є інноваційною IT-компанією, заснованою кількома особами у 2014 році, і має статутний капітал, розділений на частки відповідно до встановлених установчими документами розмірів.

Компанія є передовим гравцем на ринку IT-послуг і володіє сучасними виробничими можливостями, у тому числі, має стратегічних партнерів. Конкурує з іншими представниками IT-галузі та надає якісні послуги клієнтам.

Основна мета діяльності – задовольняння суспільних потреб у сфері інформаційних технологій та отримання прибутку в результаті господарської діяльності. Головні завдання компанії включають:

- залучення нових клієнтів до співпраці;
- розвиток та збільшення кола замовників;
- посилення співпраці з нашими постійними партнерами.

Цілі компанії «IT-House»:

- забезпечення найвищого рівня задоволення клієнтів, надаючи їм інноваційні рішення для вирішення їхніх потреб;
- постійне удосконалення продуктів і послуг, враховуючи сучасні технологічні тенденції та потреби ринку;
- розвиток та набуття глобального впливу, розширення географії послуг.

Прибуток компанії «IT-House» постійно зростає завдяки успішному впровадженню інноваційних рішень та високоякісному обслуговуванню клієнтів.

Основними видами діяльності є розробка та впровадження програмного забезпечення, інтеграція систем та розробка рішень для бізнес-автоматизації, консалтинг з питань інформаційних технологій та цифрової трансформації. Організаційна структура «IT-House» ретельно розроблена для оптимальної роботи і підтримки всіх напрямків діяльності. Вона має ефективні системи управління, які сприяють координації завдань та підвищенню продуктивності. Економічний стан компанії відзначається стійким зростанням обсягу прибутків і розширенням ринкового присутності. Компанія здатна ефективно управляти ресурсами та фінансами для досягнення цілей.

Системи менеджменту включають в себе принципи якості, безпеки та сталого розвитку. Менеджмент дотримується найвищих стандартів у всіх аспектах діяльності, що дозволяє забезпечити надійність та інноваційність рішень для клієнтів.

Економічний стан IT-компанії «IT-House» характеризується стабільним фінансовим положенням та зростаючими прибутками. ТОВ має високий рівень прибутковості завдяки успішному впровадженню інноваційних рішень та високоякісному обслуговуванню клієнтів. Компанія також має різні джерела доходу, включаючи розробку програмного забезпечення, інтеграцію систем та консалтинг.

«IT-House» представляє свою продукцію на міжнародному ринку. Підприємство має замовників з таких країн: Сполучені Штати Америки, Англія, Німеччина, Данія, Франція, ОАЕ.

Організаційна структура IT-компанії – лінійна та представлена на рисунку 2.7. Така структура відображає ієрархічну систему управління, де кожен працівник має чітко визначені обов'язки та повинен звітувати лише одному безпосередньому керівникові. В основі цієї структури лежить вертикальна система керівництва, де керівники вищого рівня видають накази та вказівки підлеглим.

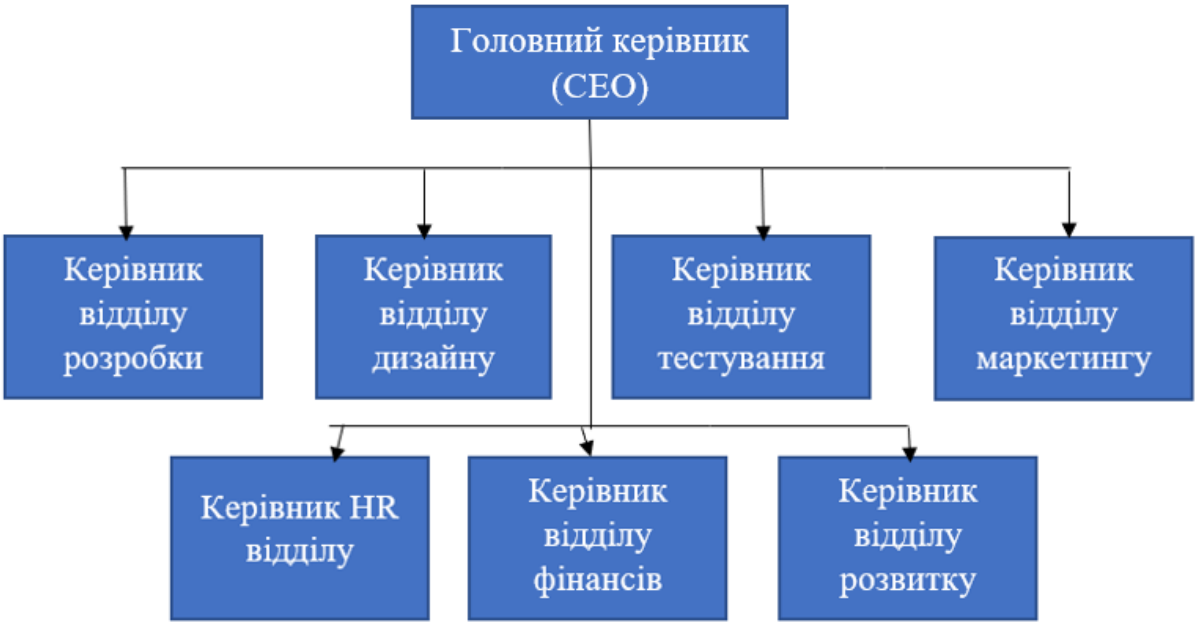

Рисунок 2.7 – Організаційна структура ТОВ «IT-House»

Для внутрішнього обліку та звіту компанія використовує свою внутрішню розробку. Це програмне забезпечення дозволяє співробітникам відстежувати та керувати своїм часом більш ефективно. Її основні функції – це деталізований облік робочого часу, планування та призначення завдань, аналіз продуктивності, інтеграція з іншими інструментами та підготовка необхідних звітів та розсилок.

Щодо виробничих процесів, «IT-House» використовує Jira як інструмент для керування проектами та робочими завданнями. Вони встановили систему відстеження завдань, розподілення робочого часу, та співпрацюють над різними етапами розробки за допомогою цієї платформи, що сприяє ефективності та координації у всій компанії. Для ілюстрації можна уявити Jira як велику дошку, розділену на секції або колонки, кожна з яких представляє певний етап роботи. Завдання (картки) переміщуються з однієї колонки в іншу, відображаючи прогрес в їх виконанні. Команди можуть спостерігати за цими завданнями, редагувати їх, надавати коментарі та відслідковувати прогрес.

2.4 Аналіз фінансово-економічного стану ТОВ «IT-House»

Ключовим елементом для забезпечення фінансово-економічної стійкості підприємства є аналіз та оцінка його фінансового стану. Цей процес ґрунтується на використанні різних показників, таких як показники фінансового здоров'я підприємства та рівень його фінансової безпеки.

Фінансовий стан підприємства відображає його здатність до саморозвитку та стан капіталу в певний момент часу під час обігу коштів.

Матеріально-технічна база підприємства – це сукупність усіх матеріальних умов, необхідних для здійснення виробничого процесу, включаючи технологічні аспекти у всіх галузях та підрозділах організації.

Основні засоби визначаються як матеріальні цінності, що забезпечують виробничий та невиробничий процес протягом тривалого періоду, перевищуючи рік у використанні.

Згідно з чинною класифікацією, основні засоби групуються в залежності від їх функціонального призначення, сфери застосування та матеріально-натуральних характеристик.

В залежності від своєї призначеності, основні засоби поділяються на дві категорії: виробничі та невиробничі.

Виробничі основні засоби безпосередньо використовуються у виробничому процесі або сприяють його здійсненню. Це включає будівлі, споруди, силові машини, устаткування, транспортні засоби, передавальні пристрої, робочу худобу, багаторічні насадження та інші засоби, які безпосередньо використовуються у матеріальному виробництві.

Невиробничі основні засоби не прямо або опосередковано використовуються у виробництві та призначені для виконання потреб житлово-комунального господарства, охорони здоров'я, освіти, культури.

Сюди відносяться споруди, будівлі, машини, обладнання, апарати та інші засоби, що застосовуються у сфері невиробничої діяльності.

У таблиці 2.1 показано склад основних засобів та його зміни впродовж 2021–2023 рр. в компанії «IT-House».

Таблиця 2.1 – Склад основних засобів компанії «IT-House» за 2021–2023 рр. (тис. грн.)

№	Показники	Значення за роками			Абсолютне відхилення		Темп росту, %	
		2021	2022	2023	2021/2022	2022/2023	2021/2022	2022/2023
1	Будинки, споруди	521,50	587,00	547,00	65,50	-40,00	112,56	93,19
2	Машини та обладнання	428,60	602,20	602,20	173,60	0,00	140,50	100,0
3	Інструменти, прилади, інвентар	249,30	528,00	560,20	278,70	32,20	211,79	106,1
4	Всього	1199,4	1717,2	1709	517,8	-7,80	464,85	299,29

Як видно з таблиці 2.1 впродовж періоду 2021–2023 рр. відбулися такі зміни: найбільш зросла вартість інструментів, приладів та інвентарю (меблів) на 310,9 тис. грн, в 2022 р. вартість транспортних засобів зросла на 60,1 тис. грн і залишилась незмінною на 2021 р., вартість машин та обладнання на протязі періоду 2021-2022 рр. по зросла на 173,6 тис. грн та теж залишалась незмінною, на кінець 2021 р. вартість будинків та споруд зросла на 25,5 тис. грн порівняно з 2021 р., та зменшилась на 40 тис. грн у порівнянні з 2022р. Загальна вартість основних засобів протягом вказаного періоду зросла на 509,6 тис. грн, що свідчить про покращення стану технічного забезпечення виробництва.

Активи відображають ресурси, які підприємство контролює в результаті минулих подій і використання яких, як очікується, призведе до отримання економічних вигід у майбутньому. Класифікація активів ґрунтується на їх складі, місцезнаходженні та ролі у процесі діяльності.

У балансі активи розділяють на необоротні, оборотні та витрати майбутніх періодів.

Оборотні активи – це грошові кошти та їх еквіваленти, що використовуються необмежено, а також інші ресурси, спрямовані на реалізацію чи споживання протягом оперативного циклу або протягом 12 місяців після балансової дати. Сюди відносяться: готівка в касі та на банківських рахунках, виробничі запаси, короткострокові фінансові інвестиції, дебіторська заборгованість (включаючи заборгованість підзвітних осіб та покупців) та витрати, які покладено на майбутні періоди, але що виникли протягом поточного або минулих періодів.

Необоротні активи – це ресурси, що мають тривалий строк корисного використання, перевищуючи один рік або оперативний цикл, що триває понад рік. Ця категорія поділяється на основні засоби, нематеріальні активи, довгострокові фінансові інвестиції та інші необоротні активи.

Динаміка складу активів та їх зміни відображені у таблиці 2.2 балансу підприємства. За наведеними даними загальна вартість активів зросла на 2 137,2 тис. грн у порівнянні з 2021 роком, але зменшилась на 1 108,5 тис. грн у порівнянні з 2022 роком.

Визначення основних видів прибутку підприємства ІТ-компанії наведено в таблиці 2.3.

Таблиця 2.2 – Склад активів ТОВ «IT-House» за 2021–2023 рр. (тис. грн)

№	Показники	Значення за роками			Абсолютне відхилення		Темп росту, %	
		2021	2022	2023	2021/2022	2022/2023	2021/ 2022	2022/ 2023
1	Необоротні активи, в тому числі:							
2	Незавершене виробництво	53,30	852,00	1236	798,70	384,00	1 598,50	145,1
3	Основні засоби	2 760,8	3 164,40	1860	403,60	-1303,8	114,62	58,80
4	Довгострокові фінансові інвестиції	96,80	219,20	149,50	122,40	-69,70	226,45	68,20
5	Довгострокова дебіторська заборгованість	13,70	146,80	52,50	133,10	-94,30	1071,53	35,76
6	Оборотні активи, в тому числі:							
7	Виробничі запаси	73,00	118,80	106,3	45,80	-12,50	162,74	89,48
8	Товари	243,40	129,90	161,8	-113,5	31,90	53,37	124,6
9	Дебіторська заборгованість	3 879,3	6 141,30	5 632,7	2 262,0	-508,60	158,31	91,72
10	Грошові кошти та їх еквіваленти	853,50	730,90	470,2	-122,60	-260,70	85,64	64,33
11	Всього	6 773,6	10 009,3	8 900,8	3 235,7	-1 108,50	147,77	88,93

Таблиця 2.3 – Визначення основних видів прибутку підприємства «IT-House» за 2021 – 2023рр. (тис. грн.)

№	Показники	Значення за роками			Абсолютне відхилення		Темп росту, %	
		2021	2022	2023	2021/2022	2022/2023	2021/2022	2022/2023
1	Дохід (виручка) від реалізації (товарів, робіт, послуг)	57 806	32 312,70	21 627,20	-25 493,30	-10 685,50	55,90	66,93
2	Податок на додану вартість	9 521,7	5 047,00	3 317,20	-4 474,70	-1 729,80	53,01	65,73
3	Чистий дохід (виручка) від реалізації продукції (товарів, робіт, послуг)	48 284	27 265,70	18 310,00	-21 018,60	-8 955,70	56,47	67,15
4	Собівартість реалізованої продукції (товарів, робіт, послуг)	45 402	25 006,10	16 450,10	-20 395,50	-8 556,00	55,08	65,78
5	Валовий прибуток	2 882,7	2 259,60	1 859,90	-623,1	-399,7	78,38	82,31
6	Інші операційні доходи	902,2	2 180,10	1 385,40	1 277,90	-794,7	241,64	63,55
7	Адміністративні витрати	1 362,4	1 342,20	976,1	-20,2	-366,1	98,52	72,72
8	Витрати на збут	461,8	529,8	425,2	68	-104,6	114,72	80,26
9	Інші операційні витрати	1 155,3	2 166,70	1 582,50	1 011,40	-584,2	187,54	73,04
10	Фінансові результати від операційної діяльності, прибуток	805,4	401	261,5	-404,4	-139,5	49,79	65,21
11	Інші доходи	15,6	40,9	306,2	25,3	265,3	262,18	1137,26
12	Фінансові витрати	171	43,1	108,6	-127,9	65,5	25,20	32,36
13	Інші витрати	72,6	31,4	357,1	-41,2	325,7	43,25	117,26
14	Фінансові результати від звичайної діяльності	316,6	225,8	102	-90,8	-123,8	71,32	45,17
15	Чистий прибуток	316,6	225,8	102	-90,8	-123,8	49,79	65,21

Прибуток, як економічний показник, піддається впливу різноманітних факторів, які можна розділити на зовнішні та внутрішні.

До зовнішніх факторів належать ті, що не залежать від самого розвитку підприємства:

- інфляційні процеси;
- законодавство;
- політика;
- науково-технічний та соціальний розвиток регіону;
- політика оподаткування та інші.

До внутрішніх факторів належать ті, що залежать від саме діяльності певного підприємства. Вони можуть впливати на формування прибутку як безпосередньо, так і опосередковано. Оцінку ступеня впливу безпосередніх факторів можна проводити за допомогою простих арифметичних розрахунків. Серед них варто відзначити такі:

- обсяги продукції, що випускається;
- собівартість виробництва;
- ціна продукції, що реалізується;
- найменування (асортимент) продукції, що випускається.

Як видно з даних, представлених в таблиці 2.3 чистий прибуток підприємства зменшується у 2022 р. порівняно з 2021 р. на 90,8 тис. грн, в 2023 р. порівняно з 2021 р. – на 123,8 тис. грн, а в 2023 р. порівняно з 2021 р. прибуток зменшився на 214,6 тис. грн. Це викликано збільшенням витрат на виробництво та зменшеннями об’ємів виробництва.

Прибуток показує результати діяльності підприємства у абсолютних значеннях, не враховуючи використані для його досягнення ресурси. Щоб отримати більш повне уявлення, слід доповнювати його показником рентабельності, що характеризує ступінь доцільності та ефективності цих результатів.

Фінансовий стан підприємства описує його здатність фінансувати власну діяльність. Він відображає наявність необхідних фінансових ресурсів для нормального функціонування, їх ефективне розподілення та використання, а також фінансові взаємовідносини з іншими суб'єктами, платоспроможність та стабільність.

Основними чинниками, що визначають фінансовий стан, є: виконання фінансового плану, поповнення оборотного капіталу за рахунок прибутку, швидкість оборотності оборотних коштів. Платоспроможність, яка виявляється у здатності вчасно виконувати платежі, є сигналом стану підприємства.

Фінансові ресурси – це загальна сума власного, позиченого та залученого капіталу, використовувана підприємством для формування активів та забезпечення виробничо-господарської діяльності з метою отримання прибутку.

Висновки до другого розділу

Фінансова стабільність компанії «IT-House» є важливою, але в сучасному бізнес-середовищі завжди існує ризик недобросовісної конкуренції. Щоб забезпечити фінансову економічну безпеку та вдосконалювати її постійно, варто розглянути наступні аспекти:

– моніторинг конкурентів: важливо слідкувати за діяльністю конкурентів, особливо тих, які можуть намагатися використовувати недобросовісні методи, такі як демпінг (продаж продуктів або послуг за цінами, що не покривають витрати). Потрібно аналізувати їх стратегії і реагувати на відповідний спосіб, наприклад, шляхом зміни ціноутворення або підвищення якості продукції;

– захист інтелектуальної власності: якщо компанія розробляє унікальні продукти чи технології, важливо забезпечити їх правовий захист через патенти, авторські права та інші форми інтелектуальної власності. Це допоможе уникнути копіювання та незаконного використання інших гравців на ринку;

– розвиток бренду: сильний бренд є важливим активом, який допомагає відокремити вашу компанію від конкурентів. Інвестування у маркетинг, рекламу та розвиток позитивного іміджу допоможе зберегти і підсилити вашу позицію на ринку;

– диверсифікація: важливо розглядати можливості для розширення бізнесу та диверсифікації доходів. Це дозволить зменшити ризик в разі втрати частини ринку через недобросовісну конкуренцію;

– партнерство та альянси: співпраця з іншими компаніями може забезпечити додатковий захист від конкурентів. Наприклад, утворення стратегічних альянсів або партнерства з іншими гравцями може допомогти об'єднати ресурси та зміцнити вашу позицію на ринку;

– інновації: постійна робота над вдосконаленням продуктів і послуг допомагає не лише захищати фінансову економічну безпеку, але і розвивати бізнес. Інновації дозволяють збільшити конкурентоспроможність і займати лідируючі позиції на ринку.

Приклади заходів, які можна вжити для захисту фінансової економічної безпеки, включають в себе патентування технологій, перевірку контрагентів на добросовісність перед укладенням угод, активну роботу зі створенням і підтримкою бренду, регулярне оновлення продукції та пошук нових ринкових можливостей. Загалом, надійна фінансова економічна безпека вимагає постійного аналізу ринкових умов та реагування на зміни, щоб забезпечити стабільність і успіх компанії.

3 УДОСКОНАЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ НЕДОБРОСОВІСНОЇ КОНКУРЕНЦІЇ

3.1 Загальні стратегії удосконалення системи забезпечення економічної безпеки

Удосконалення системи забезпечення економічної безпеки підприємства в умовах недобросовісної конкуренції – це складний процес, що передбачає вжиття ряду заходів для захисту підприємства від недобросовісних дій конкурентів та забезпечення його стійкості й стабільності на ринку.

Отримати конкретний список рекомендацій для певного підприємства можна лише після проведення аналізу його ситуації, але загальні стратегії удосконалення системи забезпечення економічної безпеки можуть включати:

– моніторинг конкуренції – слід постійно аналізувати дії конкурентів, їх стратегії та тактики для виявлення недобросовісних дій чи порушень правил гри;

– юридичний захист – використання правових засобів для захисту власної інтелектуальної власності, укладання договорів з конфіденційністю тощо;

– зміцнення бренду та репутації – підтримка позитивного іміджу компанії може зменшити вплив недобросовісних практик конкурентів;

– технологічний захист – захист технічних розробок, інновацій та конфіденційної інформації;

– партнерства та альянси – розширення співпраці з надійними партнерами може забезпечити додаткову підтримку та захист від недобросовісних конкурентів;

– навчання та розвиток персоналу – підвищення обізнаності співробітників з питань конкурентного середовища й способів захисту від недобросовісної конкуренції.

Моніторинг конкуренції – це стратегічний процес аналізу та спостереження за діяльністю конкурентів у вашій галузі. Це важливий елемент будь-якого бізнесу, оскільки дозволяє краще розуміти ринок, реагувати на зміни та виявляти можливості для покращення власної стратегії.

Одним з ключових аспектів моніторингу конкуренції є аналіз стратегій та тактик конкурентів. Це включає увесь спектр дій, що вони виконують: від маркетингових кампаній та цінової політики до використання новітніх технологій та взаємодії з клієнтами. Розуміння цих стратегій дозволяє вам не лише реагувати на їхні дії, але й знаходити у них слабкі місця або можливості для вдосконалення власного бізнесу.

Також важливою частиною моніторингу конкуренції є виявлення недобросовісних дій або порушень правил гри. Це може включати неправдиву рекламу, порушення авторських прав, недотримання стандартів безпеки або інші етичні або законодавчі витоки. Виявлення таких ситуацій дозволяє вам захистити свій бізнес від недобросовісної конкуренції та вжити заходів для вирішення цих проблем.

Для успішного моніторингу конкуренції необхідно використовувати різноманітні інструменти: від аналізу інтернет-ресурсів та соціальних мереж до збору інформації з публічних джерел або спеціалізованих програмних засобів для аналізу ринку.

Загалом, моніторинг конкуренції – це важливий елемент стратегії будь-якого бізнесу, оскільки він дозволяє краще розуміти ринок, адаптувати свої стратегії та зберігати конкурентну перевагу.

Юридичний захист в контексті бізнесу включає в себе використання правових засобів для захисту власної інтелектуальної власності та укладання договорів з конфіденційністю. Це важлива складова стратегії, що дозволяє

компаніям зберігати конкурентні переваги, захищати створені продукти, технології, бренди та інші активи.

Один з основних аспектів – це захист інтелектуальної власності. Це охоплює патенти, авторські права, товарні знаки, винаходи, дизайни тощо. Застосування правових засобів, таких як патентування або реєстрація авторських прав, дозволяє утримати ексклюзивність та контроль над тим, що було розроблено або створено компанією.

Договори з конфіденційністю є ще одним важливим аспектом. Вони встановлюють правила конфіденційності для інформації, яка передається третім особам. Це може бути важливим для захисту комерційної та технічної інформації, бізнес-планів, стратегій маркетингу тощо.

Захист інтелектуальної власності та укладання договорів з конфіденційністю часто вимагають співпраці з юридичними консультантами або адвокатами, оскільки це складні процеси, що вимагають ретельного вивчення законів та врахування специфіки кожного випадку.

Використання юридичних засобів для захисту власної інтелектуальної власності є необхідністю в умовах сучасного бізнесу, де конкуренція і швидкість інновацій зростають. Це допомагає компаніям зберегти свої активи, захистити їх від недобросовісних дій конкурентів та забезпечити стабільний розвиток бізнесу.

Технологічний захист є важливою складовою для збереження конкурентних переваг у сучасному бізнес-середовищі. Це охоплює заходи, спрямовані на захист технічних розробок, інновацій та конфіденційної інформації від несанкціонованого доступу, копіювання або використання третіми особами без дозволу.

Одним з основних аспектів технологічного захисту є забезпечення безпеки технічних розробок і інновацій. Це включає в себе застосування шифрування, внутрішніх політик безпеки, захист мережі та інших технічних заходів для запобігання несанкціонованому доступу до важливої інформації.

Крім того, технологічний захист включає в себе такі аспекти, як захист конфіденційної інформації під час передачі по мережі, зберігання на захищених серверах чи використання технологій обмеження доступу до важливих даних та інформації.

Для досягнення ефективного технологічного захисту компанії використовують спеціалізовані програмні засоби, файрволи, антивірусні програми, системи ідентифікації та аутентифікації користувачів, а також проводять регулярні аудити безпеки для виявлення потенційних вразливостей.

Ключовим аспектом технологічного захисту є постійне оновлення заходів та систем захисту, оскільки технологічні загрози постійно еволюціонують. Це вимагає постійного моніторингу та адаптації заходів захисту до нових викликів та ризиків.

У цілому, технологічний захист є критично важливим для забезпечення безпеки та конфіденційності технічних розробок, інновацій та конфіденційної інформації, що є ключовими активами багатьох сучасних компаній.

Зміцнення бренду та репутації компанії є критично важливими аспектами для успішного функціонування на ринку. Підтримка позитивного іміджу не лише сприяє залученню нових клієнтів та партнерів, але й може допомогти у зменшенні впливу недобросовісних практик конкурентів.

Зміцнення бренду включає в себе створення унікальної та запам'ятовувальної ідентичності компанії, її цінностей та продуктів. Це може бути досягнуто через ефективну маркетингову стратегію, сприятливе спілкування з аудиторією, створення якісних товарів та послуг, а також акцент на корпоративну відповідальність.

Репутація компанії – це сукупність сприйняття споживачів, партнерів та громадськості щодо її чесності, надійності та етичного ставлення. Підтримка доброї репутації вимагає постійної уваги до якості продуктів, високого рівня обслуговування клієнтів, а також відкритості та прозорості в управлінні бізнесом.

Позитивний імідж компанії може допомогти у зменшенні впливу недобросовісних практик конкурентів через кілька способів:

– довіра споживачів – якщо компанія відома своєю доброю репутацією, споживачі будуть більш схильні довіряти їй, і це може зменшити вплив негативних кампаній конкурентів;

– стійкість до криз – компанія з сильним брендом має більшу стійкість до кризових ситуацій або атак з боку конкурентів, оскільки вже має позитивний капітал довіри в очах споживачів;

– публічний опір недобросовісним діям – у разі, якщо недобросовісні практики стають відомими громадськості, компанії з сильним брендом можуть отримати підтримку споживачів, що утворить опір проти конкурентів;

– сприятливе ставлення до кризових ситуацій – якщо компанія має добру репутацію, вона може краще впоратися з кризовими ситуаціями, у тому числі й тими, які можуть бути спровоковані негативними діями конкурентів.

Таким чином, зміцнення бренду та репутації компанії не лише сприяє її успішності та залученню клієнтів, але й може допомогти у зменшенні впливу недобросовісних практик конкурентів, створюючи віру в надійність та етичність вашого бізнесу.

Ці стратегії можуть бути використані підприємствами для зміцнення своєї позиції та захисту від недобросовісних практик конкурентів.

3.2 Поточний стан системи забезпечення економічної безпеки підприємства «IT-House» в умовах недобросовісної конкуренції

Підприємство «IT-House» знаходиться в напруженій ситуації через недобросовісну конкуренцію на ринку. Останнім часом підприємство спостерігає за зростанням намагань конкурентів втручатися в їхню діяльність. Це включає в себе недобросовісні практики, такі як крадіжки конфіденційної інформації, спроби порушення контрактів або навіть недобросовісну рекламу.

Щодо моніторингу конкуренції, «IT-House» вживає активних заходів для вивчення дій конкурентів. Вони збирають і аналізують інформацію про рухи на ринку, зміни в стратегіях конкурентів та оцінюють їхній вплив на власний бізнес. Це допомагає виявляти можливі загрози та реагувати на них швидко. Компанія систематично аналізує продукти та послуги своїх конкурентів, оцінює їхні технологічні можливості, функціонал, якість та цінову політику. Цей аналіз допомагає «IT-House» розуміти сильні та слабкі сторони конкурентів, а також виявляти можливі пункти ринкової вразливості. Підприємство вивчає рекламні кампанії конкурентів, їхні маркетингові ходи та підходи до просування продуктів. Це дозволяє «IT-House» адаптувати власні стратегії, покращувати комунікацію зі своїми клієнтами та реагувати на конкурентний тиск. Постійне спостереження за ціновими змінами та пропозиціями конкурентів допомагає «IT-House» у встановленні конкурентоздатної цінової стратегії, привернені нових клієнтів та утриманні існуючих. Вивчення стратегій розвитку конкурентів допомагає «IT-House» передбачати можливі напрямки ринкового розвитку, планувати власні інновації та заходи для збереження конкурентних переваг.

У сфері юридичного захисту, «IT-House» активно співпрацює з юридичними консультантами та адвокатськими фірмами. Вони стежать за всіма порушеннями та намагаються захистити свої права через судові шляхи.

Це включає подання позовів через порушення авторських прав, порушення угод та інші недобросовісні дії конкурентів. Юридична команда «IT-House» є ключовим елементом їх стратегії захисту від недобросовісної конкуренції. Команда юристів відслідковує можливі випадки порушення авторських прав або підтвердження використання інтелектуальної власності «IT-House» без дозволу. Якщо виявляються факти порушень, вони негайно реагують, подаючи відповідні позови та вимагаючи компенсації за завданий збиток. Крім того, команда юристів стежить за виконанням угод та контрактів. Якщо конкуренти порушують умови угод або контрактів, що може завдати шкоди «IT-House», юристи вживають необхідних юридичних заходів для відновлення справедливості та вирішення цих питань через судовий процес. Крім судових заходів, юридична команда також відстоює репутацію компанії. Вони моніторять та реагують на будь-які недостовірні заяви чи наклепи, які можуть пошкодити імідж «IT-House», здійснюючи заходи для захисту честі та гідності компанії.

Щодо зміцнення бренду та репутації, «IT-House» акцентує увагу на якості своїх послуг та продуктів. Вони активно комунікують з клієнтами, намагаючись відновити довіру та демонструвати свою надійність у порівнянні з конкурентами. Крім того, підприємство розвиває стратегії маркетингу та PR для підтримки позитивного іміджу. Вони активно працюють над постійним вдосконаленням технологій, що дозволяє їм завжди залишатися на передній лінії інновацій у своїй галузі. Комунікація з клієнтами для «IT-House» – пріоритет. Вони регулярно отримують зворотній зв'язок від клієнтів, працюють над вирішенням їхніх проблем та потреб, щоб підтвердити свою увагу до клієнтів. Компанія розробляє ефективні стратегії маркетингу, спрямовані на відзначення переваг їхніх продуктів та послуг. Це може включати рекламні кампанії, участь у виставках та конференціях, спонсорство подій або випуск інформаційних матеріалів для підтримки свого бренду. Крім того, «IT-House» активно працює над своїм публічним іміджем. Вони можуть

організовувати прес-конференції, публікувати статті та думки експертів у виданнях, брати участь у панельних обговореннях для підтримки своєї авторитетності та репутації як провідного гравця у сфері.

Щодо технологічного захисту, «IT-House» вдосконалює системи кібербезпеки. Вони вкладають у заходи захисту від хакерських атак, збільшують захист конфіденційної інформації та підвищують свою стійкість до технологічних загроз. Компанія активно використовує оновлення та патчі для всього програмного забезпечення, щоб усунути вразливості та запобігти можливим атакам через виявлені вразливість. Підприємство використовує спеціальні програми та інструменти для моніторингу мережі на наявність потенційних загроз та шкідливих програм. Це допомагає вчасно виявляти та реагувати на можливі атаки. «IT-House» впроваджує заходи з кібербезпеки, такі як мережеві заходи захисту, використання фаєрволів та систем виявлення вторгнень для підвищення рівня стійкості до потенційних атак. Компанія забезпечує регулярне резервне копіювання даних та плани відновлення в разі інцидентів безпеки, щоб максимально зменшити можливі наслідки випадків атаки або втрати інформації.

Ця ситуація вимагає від «IT-House» постійного вдосконалення стратегій та відповіді на зміни у конкурентному середовищі для збереження стабільності та успішності підприємства.

3.3 Удосконалення системи забезпечення економічної безпеки підприємства «IT-House» через стратегію розвитку персоналу за допомогою програмного забезпечення та штучного інтелекту

Найбільш важливою стратегію є навчання та розвиток персоналу. Цей пункт важливий для забезпечення економічної безпеки підприємства,

особливо в умовах недобросовісної конкуренції. Це означає розробку і впровадження стратегій, спрямованих на підтримку етичності, добросовісності та відповідальності серед персоналу.

Контроль лояльності та дій персоналу є важливою складовою утримання етичної культури в компанії. Для цього можна використовувати кілька методів, які представлено на рисунку 3.1 у поєднанні зі штучним інтелектом та спеціальним програмним забезпеченням у вигляді курсів та практичних завдань.

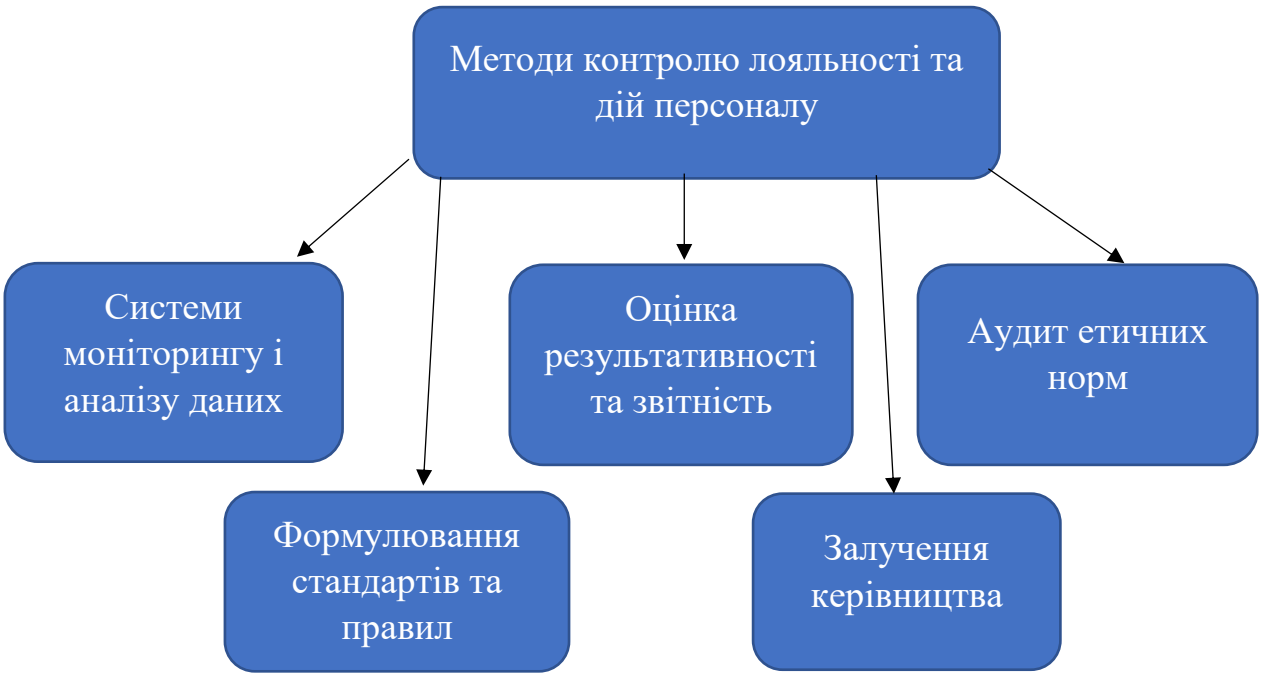

Рисунок 3.1 – Методи контролю лояльності та дій персоналу

Штучний інтелект (ШІ) у поєднанні з практичними завданнями та курсами має величезне значення для контролю лояльності та дій персоналу у багатьох сферах.

Системи моніторингу і аналізу даних – це встановлення систем, що відстежують дії персоналу. Це може бути відстеження доступу до систем, контроль за виконанням завдань або аналіз комунікацій в мережі. Штучний

інтелект може використовуватися для аналізу великих обсягів даних та виявлення аномалій у поведінці працівників.

Аудит етичних норм – це проведення періодичних аудитів для перевірки дотримання працівниками етичних стандартів. Це може бути внутрішній аудит або залучення зовнішніх консультантів.

Формулювання стандартів та правил – чітко визначені правила та стандарти етичної поведінки, які включаються до робочих контрактів або довідників для працівників. Такі стандарти допомагають керівництву в оцінці дотримання принципів.

Залучення керівництва – це активна участь топ-менеджменту у встановленні стандартів та контролі за їх дотриманням відображає важливість етичної культури для всієї компанії.

Оцінка результативності та звітність – це визначення ключових показників ефективності, включаючи етичні аспекти роботи працівників. Важливо встановити систему звітності про досягнення цих показників та регулярно аналізувати результати.

Ці заходи допомагають підтримувати та контролювати рівень дотримання етичних норм серед персоналу. Використання штучного інтелекту може полегшити цей процес шляхом автоматизації деяких етапів моніторингу та аналізу даних, забезпечуючи більш ефективний контроль та реагування на можливі порушення.

Розробка системи оцінювання результативності та звітності – це важливий процес, який вимагає кількох ключових кроків та ресурсів. Кроки для створення цієї системи викладено на рисунку 3.2.

Рисунок 3.2 – Кроки для створення системи оцінювання результативності та звітності

Визначення ключових показників успішності – це вибір показників, які найкраще відображають цілі та досягнення компанії або організації. Це можуть бути фінансові показники, якість роботи, клієнтське задоволення, етичні стандарти та інші.

Розробка механізму збору даних – це встановлення процесу збору та обробки інформації, необхідної для оцінки цих показників. Це може включати в себе внутрішні системи обліку, опитування клієнтів, відстеження виконання завдань працівниками та інше.

Важливо мати об'єктивну оцінку системи, тому залучення зовнішніх консультантів або експертів може бути корисним. Їхні знання та досвід можуть допомогти підвищити ефективність системи.

Створення системи звітності, яка включає формати звітів, графіки, таблиці та інші інструменти для візуалізації даних. Зрозуміла та доступна звітність сприяє кращому розумінню результатів.

Після впровадження системи важливо регулярно аналізувати зібрані дані, оцінювати їхню достовірність та використовувати цю інформацію для вдосконалення процесів. Новітні засоби із залученням штучного інтелекту можуть допомогти у кращому аналізі.

Створення такої системи потребує ресурсів у вигляді фінансів, часу та експертного бачення. Це може включати витрати на розробку програмного забезпечення, спеціалізовану консультацію, навчання персоналу та інше. Також важливо врахувати витрати на підтримку та вдосконалення системи з часом.

Ідея полягає в тому, що інвестиції у створення ефективної системи оцінювання та звітності можуть принести значний приріст ефективності, підвищити прозорість та етичні стандарти в організації.

Штучний інтелект дозволяє об'єктивно оцінити рівень знань, розуміння та навичок працівників в етичних питаннях. Він аналізує результати практичних завдань та курсів, надаючи точний погляд на їхню компетентність у цій області.

Також ШІ може виділяти слабкі моменти в розумінні етичних принципів серед персоналу. Це дозволяє керівництву точно побачити, де необхідно покращення або додаткова підтримка.

На основі результатів аналізу ШІ може визначити індивідуальні потреби працівників у навчанні етичних аспектів, що дозволяє створити персоналізовані програми навчання.

Аналітика, отримана за допомогою ШІ, може слугувати основою для постійного вдосконалення курсів та практичних завдань. Це дозволяє реагувати на зміни та покращувати методи навчання.

Ще за допомогою штучного інтелекту можна відстежувати динаміку змін у розумінні етичних принципів серед персоналу та відображати ці зміни в часі, допомагаючи виокремити та відстежувати покращення.

Ця інтегрована стратегія, що поєднує технології, освіту та практичні завдання, має потенціал сприяти підвищенню рівня контролю над лояльністю та етичною поведінкою персоналу. Це відображається в покращенні професійної моралі та відповідальності співробітників. В свою чергу, ці фактори сприяють підтримці фінансово-економічної стійкості компанії,

особливо в умовах недобросовісної конкуренції, через підготовку та усвідомленість персоналу.

Ця методика дозволяє компаніям систематично вдосконалювати механізми контролю над етичною поведінкою персоналу, а також підвищувати кваліфікацію працівників у сфері етики та відповідальності. Це сприяє побудові стійкого фундаменту для управління ризиками та забезпечення фінансової стабільності підприємства.

У таблиці 3.1 надано план розробки системи оцінювання результативності та звітності, який може допомогти у зручному розподілі часу та ресурсів. Створення подібного календарного плану допоможе у логічному розподілі завдань та встановленні конкретних термінів для їх виконання, що сприятиме систематичному розвитку та вдосконаленню системи оцінювання.

Також компанія повинна проводити навчання та освіту свого персоналу з питань кібербезпеки. Це включає заходи щодо посилення паролів, освіту про соціальний інжиніринг та свідоме використання технологій для уникнення фішингу. Проведення тренінгів з посилення паролів та аутентифікація. Працівники отримують навички створення сильних паролів, використання двохфакторної аутентифікації та інших методів захисту доступу до систем компанії. Ще один важливий пункт – це соціальний інжиніринг. Навчання про соціальний інжиніринг надає співробітникам знання про типові шахрайські методи, які використовуються для обману людей та отримання конфіденційної інформації. Це включає в себе заходи про фішинг, техніки впливу та методи обману через електронну пошту, соціальні мережі та телефонні дзвінки. Не менш важливим аспектом є безпека електронної пошти.

Працівники отримують інструкції щодо впізнавання підозрілих повідомлень електронної пошти, прикладів шахрайства та рекомендацій щодо безпечних практик у роботі з електронною поштою.

Таблиця 3.1 – План розробки системи оцінювання результативності та звітності

Фаза	Термін	Опис
Підготовка і планування	1-2 місяці	– Визначення мети та цілей системи: створення команди для розробки системи та визначення основних показників успішності. – Аналіз потреб: вивчення наявних ресурсів та засобів та визначення витрат на створення системи. – Планування процесу: розробка календарного плану та визначення завдань та відповідальних осіб.
Розробка системи	3-4 місяці	– Вибір показників успішності: проведення консультацій з експертами та вибір оптимальних показників. – Розробка механізму збору даних: розробка системи збору та обробки інформації, а також впровадження необхідного програмного забезпечення.
Тестування та оцінка	2 місяці	– Тестування системи: проведення тестів функціональності та коригування системи на основі отриманих результатів. – Оцінка ефективності: оцінка зібраних даних та аналіз відповідності до визначених цілей.
Впровадження та моніторинг	постійно, постійний моніторинг та покращення	– Впровадження системи: тренінг персоналу та запуск системи оцінювання. – Постійний моніторинг та вдосконалення: регулярний аналіз результатів та коригування системи для покращення ефективності.
Звітність та оптимізація	постійно, щоквартально/щорічно	– Підготовка звітів: складання звітів на основі зібраних даних. – Оптимізація системи: внесення змін до системи на основі аналізу звітів.

Компанії може також допомогти освіта про використання пристроїв та програмного забезпечення. Працівники отримують поради та навички щодо безпечного використання комп'ютерів, мобільних пристроїв та програмного

забезпечення, а також навчаються визнавати підозрілі дії на своїх пристроях. Ще один пункт – це постійне навчання та оновлення. Компанія також встановлює систему постійного навчання для персоналу з оновленнями щодо останніх загроз та методів захисту. Це може включати онлайн-курси, внутрішні тренінги та регулярні оновлення матеріалів. Ці заходи дозволяють персоналу бути більш ознайомленими та обережними щодо потенційних кіберзагроз, знижують ризики випадків атак та підвищують загальний рівень кібербезпеки в організації.

Тренування персоналу стосовно кібербезпеки — це дуже важливий напрямок. Тут є кілька способів розширити цю ініціативу. Вони представлені на рисунку 3.3.

Систематизація навчальних матеріалів	Симуляції фішингу та тестування знань	Створення "Культури Безпеки"
• Створення зручного і доступного ресурсу для співробітників, де вони можуть знайти інформацію про кібербезпеку, включаючи статті, відео, інструкції та посібники.	• Проведення симуляцій атаки фішингу, щоб перевірити, наскільки добре персонал усвідомлює ризики та реагує на них. Це також може включати тестування знань після тренувань.	• Підтримка у співробітників усвідомлення та відповідальності за кібербезпеку. Залучення до обговорень, створення регулярних брифінгів щодо останніх загроз.
Співпраця з експертами	**Моніторинг та оновлення політик безпеки**	**Подальша інтеграція заходів безпеки**
• Залучення зовнішніх експертів з кібербезпеки для проведення семінарів чи лекцій. Це може надати більше глибини та актуальності знань.	• Регулярне переглядання та оновлення політик компанії стосовно кібербезпеки з урахуванням нових загроз та технологій.	• Розгляд можливостей впровадження інших заходів, таких як захист від витоку даних, контроль доступу та інші.

Рисунок 3.3 – Способи розширення напрямків тренування персоналу стосовно кібербезпеки

Таблиця 3.2 – План введення тренувань персоналу стосовно кібербезпеки

Фаза	Термін	Опис
Підготовка	1 місяць	- Аналіз потреб: вивчення потреб персоналу щодо кібербезпеки та визначення основних аспектів, що потребують тренувань. – Формування команди: створення команди, включаючи представників від IT-відділу, HR та керівництва.
Систематизація навчальних матеріалів	2 місяці	– Вибір навчальних матеріалів: обговорення з експертами та вибір матеріалів для навчання та забезпечення доступу до онлайн-курсів та ресурсів. – Розробка курсу: створення навчальних програм для персоналу та підготовка внутрішніх матеріалів.
Симуляції фішингу та тестування знань	1 місяць	– Проведення симуляцій: введення симуляцій фішингу для перевірки реакції персоналу та збір та аналіз результатів. – Тестування знань: проведення тестувань з отриманих знань та вивчення результатів та ідентифікація слабких місць.
Створення "Культури Безпеки"	2 місяці	– Освітні заходи: проведення тренінгів та лекцій з безпеки та впровадження внутрішніх кампаній для підтримки культури безпеки. – Створення пам'яток: розробка пам'яток та інформаційних матеріалів для працівників.
Співпраця з експертами	1 місяць	– Консультації з експертами: залучення зовнішніх експертів для оцінки системи та надання порад та рекомендації щодо вдосконалення програми навчання.
Моніторинг та оновлення політик безпеки	постійно, щоквартально	– Моніторинг: встановлення системи моніторингу для відстеження успішності навчань та реакції персоналу, аналіз інцидентів та реакція на них. – Оновлення політик: періодична перегляд та оновлення політик безпеки на основі отриманих даних та змін у кіберзагрозах.
Подальша інтеграція заходів безпеки	постійно, щорічно	– Розвиток програми: постійне розширення та вдосконалення програми навчання відповідно до нових технологій та загроз. – Аудит безпеки: проведення регулярних аудитів для перевірки відповідності внутрішніх процесів стандартам безпеки.

У таблиці 3.2 надано план введення тренувань персоналу стосовно кібербезпеки. Впровадження цього плану та плану розробки системи оцінювання результативності та звітності потрібно робити після визначенням можливої вартості, яку варто занести до бюджету компанії. У вартість може закладатися програмне забезпечення або його розробка, яке необхідно для досягнення цих цілей. Також треба оцінити наявність технічного забезпечення та чи треба наймати нових працівників або є можливість реалізувати це з поточними спеціалістами.

Також можна спланувати та у подальшому закласти у бюджет продаж цієї системи іншим компаніям та отримувати прибуток від цього, так як компанія займається впровадженням програмного забезпечення.

Є ще кілька способів покращити безпеку в організації: мультифакторна аутентифікація (MFA), регулярні аудити безпеки, зашифровані засоби зберігання, створення екстрених планів дій, сегментація мережі, захист від внутрішніх загроз, резервне копіювання та відновлення даних, запобігання DDoS-атак. Так як «IT-House» це IT-компанія, то впровадження усіх цих підходів буде не таким складним як для інших компаній, бо більш вірогідно, що не треба бути навіть залучати спеціалістів ззовні. Більш детальний опис цих підходів представлено на рисунку 3.4.

Також можна ввести такі профілактичні чи запобіжні заходи щодо захисту, а саме:

– регулярні аудити та тестування безпеки: «IT-House» повинна проводити регулярні аудити та тестування безпеки для ідентифікації слабких місць у своїй інфраструктурі та програмному забезпеченні, а також для вдосконалення їх систем безпеки;

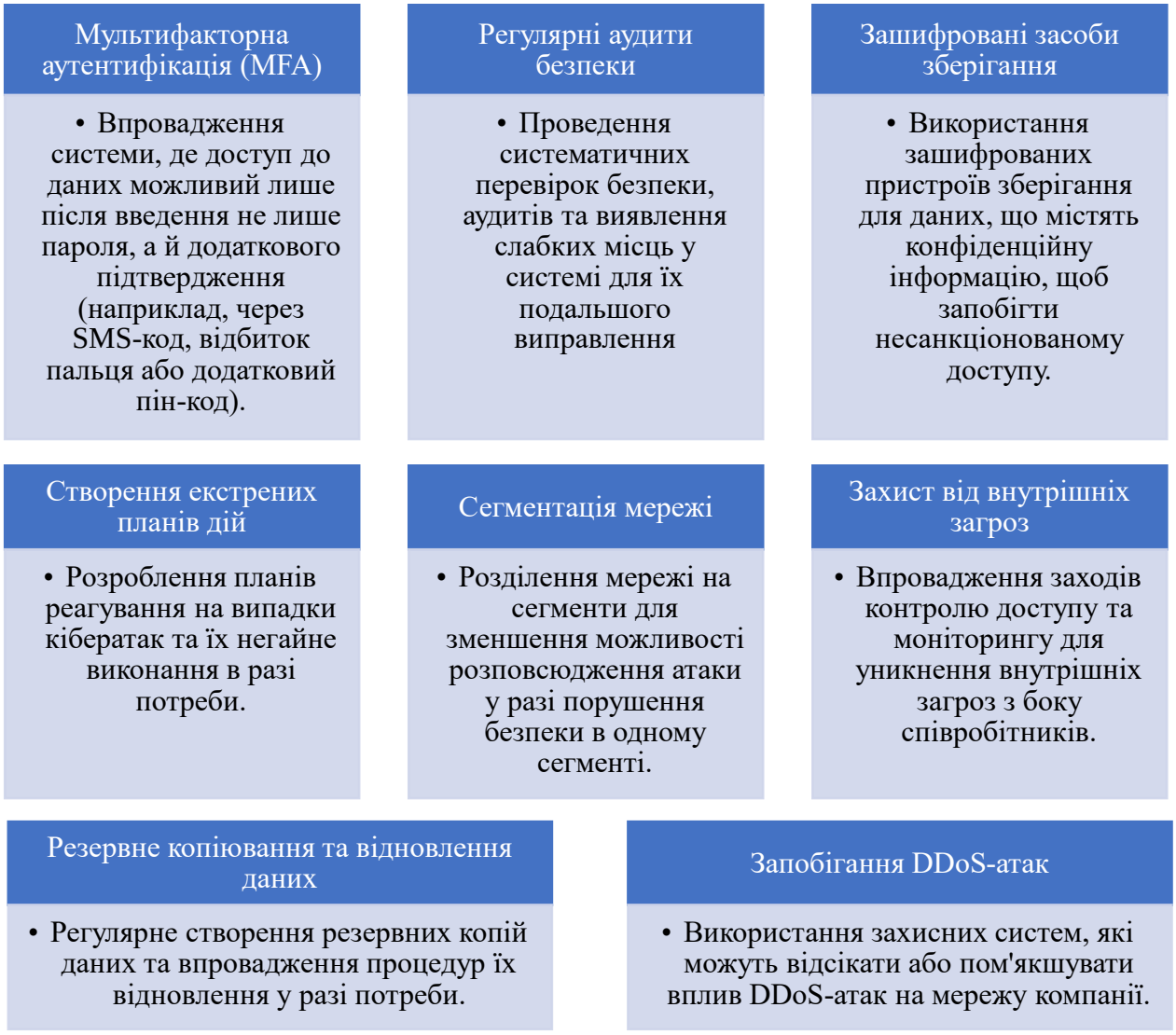

Рисунок 3.4 – Способи покращення безпеки в організації

– аудит безпеки інфраструктури: цей процес включає оцінку всіх компонентів інфраструктури компанії, таких як мережеві пристрої, сервери, зберігання даних, програмне забезпечення та інші елементи. Аудит допомагає виявити можливі слабкі місця та вразливості, такі як застарілі програми, недостатньо захищені точки доступу чи неактуальні налаштування безпеки;

– тестування вразливостей: це процес спеціальної атаки на систему або мережу компанії для ідентифікації потенційних слабкостей. Ці тести можуть включати в себе перепрограмування, сканування портів, перехоплення даних

та інші методи для виявлення вразливостей, які можуть бути використані хакерами;

– оцінка програмного забезпечення: проведення оцінки безпеки програмного забезпечення, включаючи перевірку на наявність вразливостей та можливостей усунення цих проблем через патчі та оновлення;

– оновлення політик безпеки: результати аудитів і тестувань допомагають «IT-House» вдосконалювати свої політики безпеки, щоб уникнути майбутніх проблем та підвищити рівень захисту;

– навчання та розвиток: результати аудитів служать основою для подальшого навчання персоналу та підвищення їхньої свідомості щодо кібербезпеки.

Структурно-логічна схема результатів дослідження за темою роботи (рис. 3.5) містить основні результати проведених досліджень та перелік рекомендацій щодо подальшого їх використання в обраній сфері діяльності.

Усі ці методи захисту описані у цьому розділі допоможуть компанії «IT-House» зберігати актуальну та стійку систему безпеки, постійно покращувати заходи захисту, не опинитись у скрутній ситуації. Вони дозволяють вчасно виявляти та усувати вразливості, що зменшує ризики інцидентів у майбутньому, захистити себе від недобросовісної конкуренції, залишатись у фінансовій стабільності та розвиватись незважаючи на намагання конкурентів втручатися у їхню діяльність. Також у подальшому є можливість перетворити таку систему безпеки на свій програмний продукт та продавати, щоб отримувати прибуток.

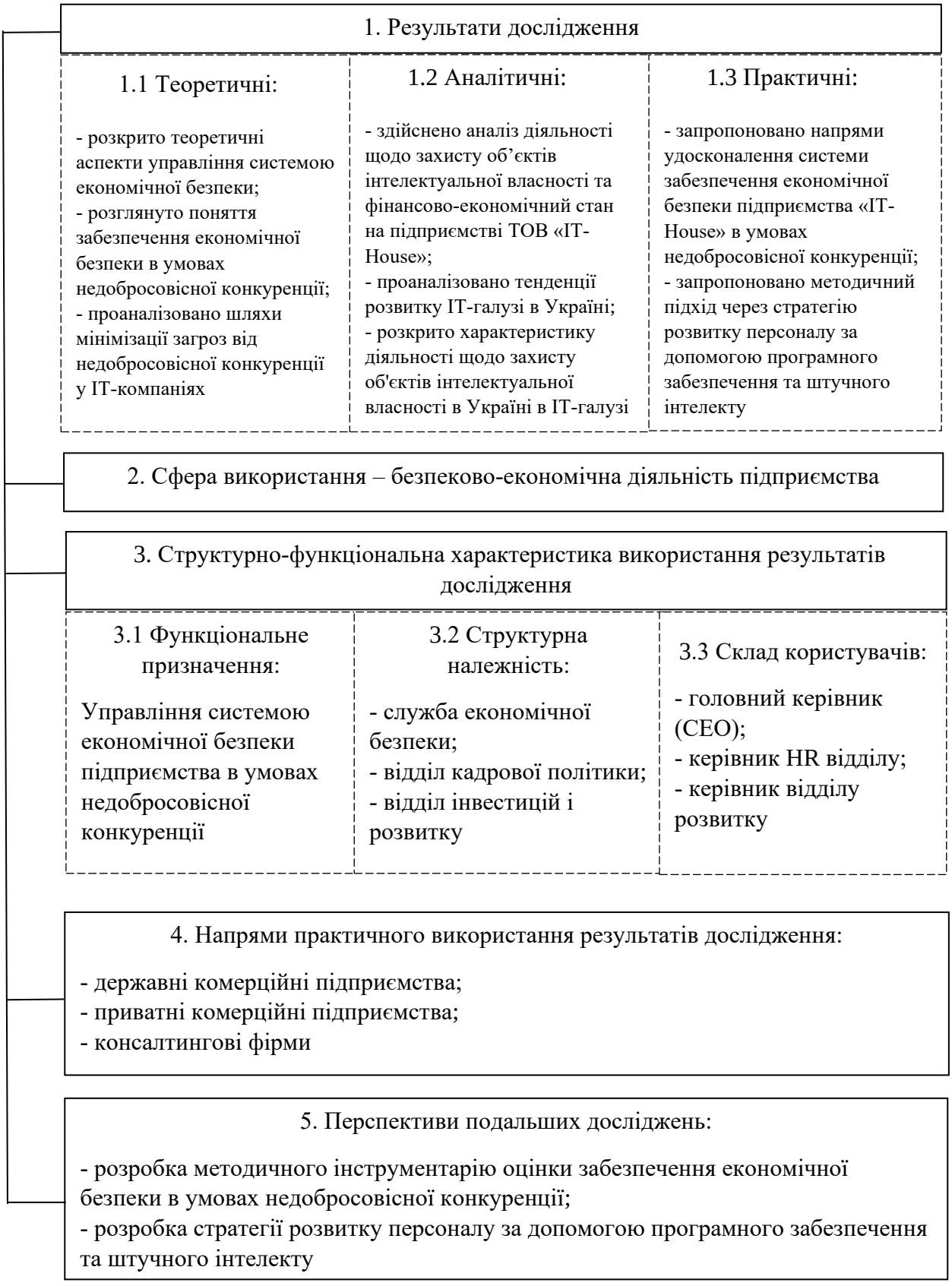

Рисунок 3.5 – Структурно-логічна схема результатів дослідження

Висновки до третього розділу

Удосконалення системи забезпечення економічної безпеки підприємства в умовах недобросовісної конкуренції – це складний процес, що передбачає вжиття ряду заходів для захисту підприємства від недобросовісних дій конкурентів та забезпечення його стійкості й стабільності на ринку.

Для успішного моніторингу конкуренції необхідно використовувати різноманітні інструменти: від аналізу інтернет-ресурсів та соціальних мереж до збору інформації з публічних джерел або спеціалізованих програмних засобів для аналізу ринку.

Підприємство «IT-House» знаходиться в напруженій ситуації через недобросовісну конкуренцію на ринку. Останнім часом підприємство спостерігає за зростанням намагань конкурентів втручатися в їхню діяльність. Це включає в себе недобросовісні практики, такі як крадіжки конфіденційної інформації, спроби порушення контрактів або навіть недобросовісну рекламу.

У третьому розділі було надано поточний стан системи забезпечення економічної безпеки підприємства «IT-House». Ситуація вимагає від «IT-House» постійного вдосконалення стратегій та відповіді на зміни у конкурентному середовищі для збереження стабільності та успішності підприємства.

Було запропоновано план та кроки для удосконалення системи забезпечення економічної безпеки підприємства «IT-House» через стратегію розвитку персоналу за допомогою програмного забезпечення та штучного інтелекту.

ВИСНОВКИ

У висновках дослідження управління фінансово-економічною безпекою в умовах недобросовісної конкуренції, можна сформулювати наступні більш розгорнуті висновки.

Завдяки аналізу сучасного ринку інформаційних технологій (IT), ми розуміємо, що це середовище відзначається високою конкурентністю та постійними змінами. Для підприємств це означає, що вони повинні бути готові до викликів та загроз, які можуть виникнути в будь-який момент.
Недобросовісна конкуренція є серйозною загрозою для IT-компаній і може включати в себе різні антиконкурентні практики, такі як демпінг, порушення прав інтелектуальної власності, або навіть поширення дезінформації. Ці практики можуть покласти під загрозу фінансову стійкість та репутацію компаній.

Управління системою економічної безпеки в умовах недобросовісної конкуренції стає критично важливим аспектом успішного функціонування підприємства. Це включає в себе ідентифікацію ризиків та розробку стратегій їх запобігання та управління.

Важливим елементом управління фінансово-економічною безпекою є захист бренду та інтелектуальної власності компанії. Це може бути досягнуто через патентування технологій, авторські права та активний моніторинг їх порушень.

Диверсифікація бізнесу і знаходження нових ринкових можливостей допомагають зменшити ризики, пов'язані з недобросовісною конкуренцією. Пошук альтернативних джерел доходу робить компанію менш залежною від одного ринку чи клієнта.

Партнерства та стратегічні альянси можуть зміцнити позицію компанії на ринку та допомогти в боротьбі з недобросовісною конкуренцією, об'єднуючи ресурси та знання.

Загальний висновок дослідження показує, що фінансово-економічна безпека ІТ-компаній в умовах недобросовісної конкуренції є критично важливою для їхнього успіху. Інформація та рекомендації, наведені в даному дослідженні, можуть бути корисними не лише для ІТ-підприємств, але і для будь-яких інших компаній, які стикаються з подібними викликами у своїй галузі.

Методи описані у останньому розділі дозволяють вчасно виявляти та усувати вразливості, що зменшує ризики інцидентів у майбутньому, захистити себе від недобросовісної конкуренції, залишатись у фінансовій стабільності та розвиватись незважаючи на намагання конкурентів втручатися у їхню діяльність. Також у подальшому є можливість перетворити таку систему безпеки на свій програмний продукт та продавати, щоб отримувати прибуток.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Великий тлумачний словник сучасної української мови : уклад. І голов. ред. В.Т. Бусел. Київ: Перун, 2009. 1736 с.

2. Бабіна Н. О. Управління економічною безпекою підприємства в умовах нестабільності. Економіка і управління. 2016. 53 с.

3. Cut Throat Competition – But Businesses Must Play Fair. URL: https://www.tutor2u.net/_legacy/assets/cafe/0905_competition_smes.pdf.

4. Полозова Т. В. Сучасні стратегії економічного розвитку: Наука, інновації та бізнес-освіта. *Матеріали ІІІ Міжнародної науково-практичної конференції*. Наук. Конф. Харків, 2022, 25-103 с.

5. Ліпкан В. А. Безпекознавство: навч. посіб. К.: Європ. ун-т., 2003. 208 с.

6. Ладико Л. Н. Механізм забезпечення економічної безпеки підприємства: сутність та структура. *Науковий вісник Полтавського університету економіки і торгівлі*. *Серія: Економічні науки.* 2014. № 3. С.123-126

7. Ілляшенко О. В. Методологічні засади формування та функціонування механізмів системи економічної безпеки підприємства: диссертація, док. екон. наук: 08.00.04 / Сєвєродонецьк, 2016. 604 с.

8. Коковський Л. О. Географічний вимір економічної безпеки України: автореф. дис... канд. геогр. наук: 11.00.02. Київ., 2008. 18 с.

9. Герасимчук З. В., Вавдіюк Н. С. Економічна безпека регіону: діагностика та механізм забезпечення: монографія. Луцьк:Надстир’я, 2006. 244 с.

10. Амельницька О. В. Управління виробничо-господарською діяльністю локальних електричних мереж: автореф. дис... канд. екон. наук: 08.00.04. Донецьк, 2008. 20 с.

11. Про захист від недобросовісної конкуренції: Закон України від 07.06.96, № 236/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/236/96-вр#Text

12. Про ринки капіталу та організовані товарні ринки: Закон України від 23.02.2006, № 3480-ІУ URL: https://zakon.rada.gov.ua/laws/show/3480-15#Text

13. Цивільний кодекс України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

14. Патентування програмного забезпечення ІТ компаніями в Україні. URL: https://wisegroup.com.ua/ua/patentuvannya-kompaniyami-svo%D1%97x-rozrobok-v-ukra%D1%97ni/

15. Станкевич Н. А. Сутність економічної безпеки підприємства. URL: https://conf.ztu.edu.ua/wp-content/uploads/2017/01/207.pdf.

16. Колот А. М. Мотивація персоналу. URL: https://polka-knig.com.ua/article.php?book=582&article=30137

17. Українська ІТ-галузь під час війни: де шукати роботу програмістам та чого очі-кувати від ринку у 2023 році? [Електронний ресурс] //AIN.UA. – URL: https://ain.ua/2022/11/01/ukrayinska-it-galuz-pid-chas-vijny-ta-pislya-de-shukaty-robotu-programistam-ta-chogo-ochikuvaty-vid-rynku-u-2023-roczi

18. Хищенко О. ІТ-ринок України: хто працює в найдинамічнішій галузі країни? – РБК-Україна [Електронний ресурс] / Олександр Хищенко / / РБК-Україна. URL: https://daily.rbc.ua/rus/show/it-rynok-ukrainy-rabotaet-samoy-dinamichno1614070059.html

19. Великий огляд IT в Україні: експорт послуг на $5 млрд щорічно, зарплати до $6000 на місяць, тарифи компаній – до $40 за годину. [Електронний ресурс] // AIN.UA. – URL: https://ain.ua/2021/04/06/obzor-it-rynka-beetroot

20. Дудко В. Український IT-експорт досягує 2022 року рекордних $7,3 млрд. Чому це насправді не дуже добра новина – Forbes.ua [Електронний ресурс] / Валентина Дудко // Forbes.ua. Бізнес, мільярдери, новини, фінанси, інвестиції, компанії. – URL: https://forbes.ua/innovations/ukrainskiy-it-eksport-dosyag-u-2022-rotsi-rekordnikh-73-mlrd-chomu-tse-naspravdi-ne-duzhe-dobra-novina-31012023-11420

21. Черненко, Н. І. Штучний інтелект в управлінні персоналом. Таврійський науковий вісник. Серія: економіка. URL: https://doi.org/10.32851/2708-0366/2022.12.11

22. Балановська Т. І., Михайліченко М. В., Троян А. В. Сучасні технології управління персоналом: навчальний посібник. Київ: ФОП Ямчинський О.В., 2020. 102с.

23. Шкробот М.В. Сучасні технології управління персоналом: навчальний посібник, Київ, 2022. 246 с.

24. Бехтер Л. А. Механізм забезпечення економічної безпеки підприємства. *Зимові читання, присвячені ідеям П. П. Німчинова та І. В. Малишева*: тези доп. X Всеукр. наук. конф. Житомир, 2012. С. 138-139.

25. Кирієнко А. Механізм досягнення і підтримки економічної безпеки підприємства: автореф. дис. канд. екон. наук : спец. 08.06.01 «Економіка, організація і управління підприємствами» / Київський національний економічний університет. Київ, 2000. 19 с.

26. Економічна безпека підприємства: підручник/ [А. М. Дідик та ін. НУ «Львівська політехніка», ТзОВ «Видавнича група «Бухгалтери України», 2019. 624 с.

27. Швидка Т. І. Боротьба з виявами недобросовісної конкуренції: проблеми законодавчого регулювання в Україні. Право та державне управління. 2021. No 1. С. 52-58. URL: http://pdu-journal.kpu.zp.ua/archive/1_2021/10.pdf

28. Кохан Д. О. Недобросовісна зовнішня конкуренція та методи захисту від неї національного ринку : автореф. дис... канд. екон. наук: 08.01.01 / Київський національний економічний ун-т ім. Вадима Гетьмана. К., 2006.

29. Гороховська О. В., Семенюк І. С. Захист комерційної таємниці в міжнародному праві та законодавстві зарубіжних країн. *Держава та регіони. Серія «Право»*. 2016. No 1. 86–91 с.

30. Про захист від недобросовісної конкуренції: Закон України від 07.06.96, No 236/96-ВР.URL: https://zakon.rada.gov.ua/laws/show/236/96-вр#Text

31. Про ринки капіталу та організовані товарні ринки: Закон України від 23.02.2006, No 3480-IУ URL: https://zakon.rada.gov.ua/laws/show/3480-15#Text

32. Цивільний кодекс України від 16.01.2003р No 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

33. Експорт українських IT-послуг у липні 2023 року перевищив минулорічні показники. DOU.UA. URL: https://dou.ua/lenta/news/it-export-july-2023/

34. Кого звільняють і де легше знайти нову роботу. Що відбувається на ринку IT в Україні. SPEKA.MEDIA. URL: https://speka.media/kogo-zvilnyayut-i-de-legse-znaiti-novu-robotu-shho-vidbuvajetsya-na-rinku-it-v-ukrayini-9d5y0v

35. Розвиток IT в Україні: поточна ситуація та перспективи. RUBRYKA.COM. URL: https://rubryka.com/blog/rozvytok-it-v-ukrayini/

36. Річний звіт УкрПатент у 2021 році. ukrpatent.org. URL: https://ukrpatent.org/atachs/zvit-ukr-2021.pdf

37. Річний звіт Антимонопольного комітету України у 2022 році. amcu.gov.ua. URL: https://amcu.gov.ua/storage/app/uploads/public /641/87f/ e95/64187fe957f1c745683055.pdf

38. Степаненко С. В., Забелін Є. Ю. Управління системою економічної безпеки ІТ-компанії в умовах недобросовісної конкуренції. Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта. Матеріали IV Міжнародної науково-практичної конференції (м. Харків, 1 листопада 2023 р.) / За заг. ред. Т. В. Полозової [та ін.]. Харків. ХНУРЕ. 2023. 171-173 с.