МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ФАКУЛЬТЕТ МІЖНАРОДНОЇ ЕКОНОМІКИ І ПІДПРИЄМНИЦТВА

КАФЕДРА ПІДПРИЄМНИЦТВА І ТОРГІВЛІ

Рівень вищої освіти	Другий (магістерський)
Спеціальність	Підприємництво, торгівля та біржова діяльність
Освітня програма	Підприємництво, торгівля та біржова діяльність
Група	8.06.076.010.22.1

ДИПЛОМНА РОБОТА

на тему: «Запровадження проєкту посилення інформаційної безпеки суб’єкта підприємницької діяльності»

Виконав: студент Євгеній ІППОЛІТОВ

Керівник: д.е.н., професор Олена ЧУПИР

Рецензент: директор ТОВ «Інтеренерго Інжиніринг»
Олександра КЛЮЄВА

Харків – 2023 рік

РЕФЕРАТ

ІППОЛІТОВ Є.М. Запровадження проєкту посилення інформаційної безпеки суб'єкта підприємницької діяльності. Дипломна робота на здобуття освітнього ступеня «магістр» зі спеціальності 076 «Підприємництво, торгівля та біржова діяльність». Харківський національний економічний університет ім. С. Кузнеця, Харків, 2023 р.

Обсяг – 92 стор.; 14 іл.; 29 табл.; 53 літературних джерела.

Метою дипломної роботи є теоретичне обґрунтування процесу забезпечення інформаційної безпеки суб'єкта підприємницької діяльності та розробка проєкту щодо її посилення на досліджуваному підприємстві.

Для досягнення мети поставлено та вирішено наступні завдання:

проведено теоретичне узагальнення поняття «інформаційна безпека»;

проведено комплексний аналіз діяльності ТОВ «Інтеренерго Інжиніринг»;

проаналізовано основні техніко-економічні показники діяльності ТОВ «Інтеренерго Інжиніринг»;

здійснено оцінювання рівня інформаційної безпеки ТОВ «Інтеренерго Інжиніринг»;

запропоновано заходи щодо підвищення рівня інформаційної підприємства.

Об'єкт дослідження – процес запровадження проєкту посилення інформаційної безпеки суб'єкта підприємницької діяльності.

Предметом дослідження є проєкт посилення інформаційної безпеки суб'єкта підприємницької діяльності.

Для реалізації даного дослідження використано загальнонаукові (теоретичного узагальнення, аналіз, синтез, індукція) і спеціально-наукові методи дослідження (економічний та фінансовий аналізи, графічний, SWOT-аналіз та ін.).

Дослідження наукової літератури, нормативно-правових актів, Законів України формують теоретичну та методичну базу дипломної роботи

Практична складова дипломної роботи базується на фінансовій та статистичній звітності суб'єкта підприємницької діяльності, на внутрішніх нормативних документах, даних бухгалтерського обліку та інформації про досліджуване підприємство.

Результати дослідження дипломної роботи були оприлюднені на IV Міжнародній науково-практичній конференції «Стратегічні пріоритети розвитку підприємництва, торгівлі та біржової діяльності» та VII Всеукраїнській науково-практичній інтернет-конференції «Перспективи розвитку управлінських систем у соціальній та економічній сферах України: теорія і практика».

Ключові слова: інформаційна безпека, зовнішні загрози інформаційної безпеки підприємства, внутрішні загрози інформаційної безпеки підприємства, диджиталізація, захист інформаційної безпеки, ризики інформаційної безпеки.

ABSTRACT

IPPOLITOV Ie. M. Implementation of the project to strengthen the information security of the business entity. Master's degree thesis for «Entrepreneurship, trade and exchange activities». S. Kuznets Kharkiv National University of Economics, Kharkiv, 2023.

Thesis contains: 92 pages; 14 figures; 29 tables; 53 literary sources.

The aim of the thesis is the theoretical substantiation of the process of ensuring the information security of the subject of entrepreneurial activity and the development of a project to strengthen it at the enterprise under study.

To achieve the goal, the following tasks were set and solved:

a theoretical generalization of the concept of "information security" was carried out;

a comprehensive analysis of the activities of "Interenergo Engineering" LLC was carried out;

the main technical and economic indicators of the activity of "Interenergo Engineering" LLC were analyzed;

assessment of the level of information security of "Interenergo Engineering" LLC was carried out;

proposed measures to increase the level of the information enterprise.

The object of the study is the process of implementing a project to strengthen the information security of a business entity.

The subject of the study is a project to strengthen the information security of the subject of entrepreneurial activity.

To implement this research, general scientific (theoretical generalization, analysis, synthesis, induction) and special scientific research methods (economic and financial analyses, graphic, SWOT analysis, etc.) were used.

The study of scientific literature, normative legal acts, Laws of Ukraine form the theoretical and methodological basis of the thesis.

The practical component of the thesis is based on the financial and statistical reporting of the subject of entrepreneurial activity, on internal regulatory documents, accounting data and information about the investigated enterprise.

The results of the thesis research were made public at the IV International Scientific and Practical Conference "Strategic Priorities of the Development of Entrepreneurship, Trade and Exchange Activity" and the VII All-Ukrainian Scientific and Practical Internet Conference "Prospects for the Development of Management Systems in the Social and Economic Spheres of Ukraine: Theory and Practice".

Keywords: information security, external threats to enterprise information security, internal threats to enterprise information security, digitalization, information security protection, information security risks.

ЗМІСТ

ВСТУП

На сьогоднішній день, в умовах постійного розвитку технологій та зростаючої кількості кіберзагроз, питання забезпечення інформаційної безпеки підприємств стає вкрай актуальним для суб'єктів підприємницької діяльності. З зростанням обсягу цифрової інформації на підприємствах зростає ймовірність кібератак та нечесного використання цієї інформації. Ефективний захист цих даних стає стратегічною необхідністю. Крім того, значна кількість країн впроваджують нові законодавчі норми, що стосуються захисту персональних даних та іншої конфіденційної інформації. Невиконання цих вимог може призвести до серйозних правових наслідків. Через те, що кіберзлочинці постійно вдосконалюють свої методи атак, тому підприємства повинні постійно вдосконалювати свої системи захисту для виявлення та протидії новим загрозам. Не треба забувати й проте, що зараз інформація стає ключовим активом бізнесу, і втрата або пошкодження цієї інформації може призвести до серйозних фінансових втрат і втрати репутації. Також зростає кількість атак, спрямованих на працівників компаній (наприклад, соціальний інжиніринг). Забезпечення безпеки включає в себе не лише технічні, але і організаційні заходи для захисту від таких загроз.

Враховуючи ці фактори, реалізація проєктів з посилення інформаційної безпеки є стратегічною необхідністю для забезпечення стійкості та надійності діяльності суб'єкта підприємницької діяльності в складно передбачуваних умовах сучасного бізнес-середовища.

Метою дипломної роботи є теоретичне обґрунтування процесу забезпечення інформаційної безпеки суб’єкта підприємницької діяльності та розробка проєкту щодо її посилення на досліджуваному підприємстві.

Для досягнення мети поставлено та вирішено наступні завдання:

проведено теоретичне узагальнення поняття «інформаційна безпека»;

проведено комплексний аналіз діяльності ТОВ «Інтеренерго Інжиніринг»;

проаналізовано основні техніко-економічні показники діяльності ТОВ «Інтеренерго Інжиніринг»;

здійснено оцінювання рівня інформаційної безпеки ТОВ «Інтеренерго Інжиніринг»;

запропоновано заходи щодо підвищення рівня інформаційної підприємства та оцінено їх економічну ефективність з урахуванням ризиків.

Об'єкт дослідження – процес запровадження проєкту посилення інформаційної безпеки суб'єкта підприємницької діяльності.

Предметом дослідження є проєкт посилення інформаційної безпеки суб'єкта підприємницької діяльності.

Для реалізації даного дослідження використано загальнонаукові (теоретичного узагальнення, аналіз, синтез, індукція) і спеціально-наукові методи дослідження (економічний та фінансовий аналізи, SWOT-аналіз та ін.).

Дослідження наукової літератури, нормативно-правових актів, Законів України формують теоретичну та методичну базу дипломної роботи.

Практична складова дипломної роботи базується на фінансовій та статистичній звітності суб'єкта підприємницької діяльності, на внутрішніх нормативних документах, даних бухгалтерського обліку та інформації про досліджуване підприємство, яка наведена на сайті.

Результати дослідження дипломної роботи були оприлюднені на IV Міжнародній науково-практичній конференції «Стратегічні пріоритети розвитку підприємництва, торгівлі та біржової діяльності» (дод. А) та VII Всеукраїнській науково-практичній інтернет-конференції «Перспективи розвитку управлінських систем у соціальній та економічній сферах України: теорія і практика».

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

1.1. Інформаційна безпека як об'єкт дослідження

Сучасний етап розвитку українського суспільства характеризується постійним зростанням важливості ролі інформаційної сфери підприємств, що представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, формування, поширення та використання інформації, а також системи регулювання громадських відносин, що виникають при цьому.

Об'єктивна необхідність у формуванні системи інформаційної безпеки підприємства виникає внаслідок низки певних чинників. Першим чинником є зростання інформації у діяльності підприємства. В умовах інформаційного суспільства інформаційні технології знайшли широке використання у виробництві: у поступовому переході від паперового документообігу до цифрового. Швидкий розвиток інформаційних технологій призводить до розповсюдження використання комп'ютерних засобів та об'єднання їх у мережі, що у рази полегшує завдання обробки, обміну та доступу до інформації для кожного суб'єкта підприємницької діяльності.

Необхідно зауважити, що спрощення доступу поширюється також на ринкових конкурентів та інших осіб, які можуть використовувати інформацію підприємства у протиправних цілях. Інформація отримала економічну роль – стала ресурсом, товаром та послугою. Виник сектор виробництва інформації, у якому завдання інформаційної безпеки мають ще більше значення. Ці чинники зумовили значне зростання зацікавленості підприємств до створення комплексних систем інформаційної безпеки.

При неправильній організації умов інформаційної безпеки створюється середовище для появи її загроз – подій, дій, процесів та явищ, які можуть

призвести до втрати конфіденційності, цілісності та/або доступності інформації.

Захист інформації є необхідним у зв'язку здатністю управлінських органів підприємства на різних рівнях з метою:

забезпечити стійкий економічний розвиток підприємства;

нейтралізувати негативний вплив кризових явищ у економіці;

сформувати адекватну систему обліку фінансових потоків та зміцнити операційну ефективність системи контролю;

забезпечити виконання робіт з захисту конфіденційності інформації, включаючи комерційну таємницю та інші аспекти.

Через зростання рівня використання інформаційних ресурсів і реальністю численних загроз стає вельми актуальною потреба у глибокому вивченні проблеми інформаційної безпеки підприємств і організацій в Україні. Без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку. Зростання обсягів фінансових та організаційних ресурсів для захисту інформації, разом з існуючими недоліками у звичайних методах реалізації системи захисту інформації, призводить до збільшення навантаження на персонал підприємства та затримки у процесі управлінських рішень.

Поняття інформаційної безпеки в різних сутнісних контекстах розглядається з декількох позицій. За загальним розумінням, інформаційна безпека представляє собою стан захищеності інформаційного середовища суспільства, сприяючи його формуванню, використанню та розвитку в інтересах громадян, організацій та держави.

Під інформаційним середовищем розуміється сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням і споживанням інформації. Інформаційне середовище можна умовно поділити на три основні частини:

1) створення та розповсюдження інформації – включає в себе процеси створення та поширення вихідної та похідної інформації;

2) формування інформаційних ресурсів - обумовлено підготовкою інформаційних продуктів, наданням інформаційних послуг та створенням інформаційних ресурсів;

3) споживання інформації – включає в себе активності, пов'язані зі споживанням інформації.

До забезпечувальної складової також входять такі:

1) створення і застосування інформаційних систем та технологій – включає процеси створення та використання інформаційних систем, технологій та їхнє забезпечення;

2) створення і застосування засобів і механізмів інформаційної безпеки – обумовлено впровадженням засобів та механізмів, що забезпечують інформаційну безпеку.

Все вище зазначене дає можливість надати більш розгорнуте визначення інформаційної безпеки – це стан захищеності потреб у інформації особистості, суспільства та держави, який забезпечує їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Важливо відзначити, що задоволення будь-якої потреби в інформації призводить до засвоєння відомостей про навколишній світ і процеси в ньому, тобто до інформованості особистості, суспільства і держави. Ступінь інформованості визначає адекватність сприйняття суб'єктами навколишньої дійсності і, отже, обґрунтованість прийнятих рішень та дій.

Залежно від виду загроз, інформаційну безпеку можна розглядати з таких позицій як:

захист стану особистості, суспільства, держави від впливу неякісної інформації;

захист інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;

захист інформаційних прав і свобод громадянина.

Необхідно відзначити, що в науковій літературі відсутній єдиний погляд на сутність поняття "інформаційна безпека". Для деяких авторів це поняття визначає діяльність чи стан, тоді як для інших – властивість, процес, функція чи система гарантій, здатність. Крім того, відсутня загальноприйнята норма, яка б містила дефініцію поняття "інформаційна безпека", враховуючи відмінність між поняттями "інформаційна безпека" та "безпека інформації".

Теоретичний поглиблений аналіз даного поняття наведено в табл. 1.1.

Таблиця 1.1.

Аналіз розуміння дефініції «інформаційна безпека» науковцями

Автор, джерело	Визначення поняття
1	2
Барановськии О. І. [3]	стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації и несанкціоноване її поширення и використання, а також через негативний інформаційний вплив і негативні наслідки функціонування інформаційних технологій
Богуш В. [4]	стан захищеності інформаційного середовища, який відповідає інтересам держави и забезпечується формування, використання та можливості роз-витку незалежно від впливу внутрішніх і зовнішніх інформаційних загроз
Жарков Я. М., Бєсєдіна Л. М. [20]	стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень і захист інформаційних ресурсів країни
Калюжнии Р. [39]	стан захищеності інформаційного простору, який забезпечує формування й розвиток цього простору в інтересах особистості, суспільства та держави
Кормич Б. [26]	стан захищеності встановлених законодавством норм і параметрів інформаційних процесів і відносин, що забезпечує необхідні умови існування держави, людини й суспільства як суб’єктів цих процесів і відносин

Закінчення табл. 1.1.

1	2
Ліпкан В. А., Максименко Ю. Є., Желіховськии В. М. [29]	стан захищеності життєво важливих інтересів особи, суспільства и держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації , через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації
Ортинськии В.Л., Керницькии І. С., Живко З. Б. [19]	стан захищеності інформаційного простору, який забезпечує формування й розвиток цього простору в інтересах особистості, суспільства та держави
Марущак А. І. [33]	стан захищеності життєво важливих інтересів особистості, суспільства и держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту, несвоєчасність, недостовірність інформації чи негативний інформаційний вплив, через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації
Петрик В. [38]	стан захищеності особи, суспільства и держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний , соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають ї м суттєвої шкоди

В інформаційному праві, з погляду інформаційного законодавства, інформаційна безпека розглядається як аспект інформаційних відносин, спрямований на захист життєво важливих інтересів особистості, суспільства та держави. Основна увага зосереджується на визначенні та усуненні погроз через застосування правових засобів [1, 10, 11].

Питання інформаційної безпеки, як розглядаються в юридичній та спеціальній літературі, базуються на розумінні інформаційної безпеки як складової національної безпеки України. В даному контексті важливим є завдання мінімізації шкоди, спричиненої неповнотою, несвоєчасністю або недостовірністю інформації, а також негативним інформаційним впливом через функціонування інформаційних технологій та незаконне поширення інформації [2, 26, 39].

Це обґрунтовано тим, що інформаційна безпека передбачає існування визначених державних інститутів і умов для її суб'єктів, які встановлені міжнародним та внутрішнім законодавством [3].

Зокрема, інформаційна безпека повинна бути гарантована за допомогою цілісної державної програми, яка відповідає Конституції України та чинному законодавству України, а також нормам міжнародного права. Це досягається шляхом реалізації відповідних доктрин, стратегій, концепцій та програм, пов'язаних із національною інформаційною політикою України [11, 20].

Тому можна стверджувати, що інформаційна безпека охоплює можливість безперешкодної реалізації суспільством і окремими його членами конституційних прав, пов’язаних з можливістю вільного одержання, створення та поширення інформації. Поняття інформаційної безпеки також повинно розглядатися в контексті:

- забезпечення відповідних безпечних умов існування інформаційних технологій, включаючи питання захисту інформації;
- безпеки інформаційної інфраструктури держави;
- розвитку і створення умов для існування та розвитку інформаційних процесів.

Необхідний рівень інформаційної безпеки забезпечується за допомогою комплексу політичних, економічних та організаційних заходів, спрямованих на попередження, виявлення і нейтралізацію обставин, факторів і дій, які можуть завдати шкоди або перешкодити реалізації інформаційних прав, потреб і інтересів країни та її громадян.

За словами Маркіної І. А., що під час побудови моделі управління інформаційною безпекою вона повинна дотримуватися загальноприйнятих концептуальних принципів, які закладені при створенні будь-якої системи захисту інформації. Враховуючи основні тенденції в сфері забезпечення захисту інформації при управлінні інформаційною безпекою, пропонується дотримуватися таких концептуальних принципів, серед яких такі [32]:

– законність, дотримання балансу інтересів особи, суспільства и держави;

– системність;

– плановість;

– комплексність;

– безперервність;

– взаємна відповідальність суб’єктів забезпечення інформаційної безпеки, їх взаємодія;

– спадкоємність і безперервність вдосконалення;

– розумна достатність;

– персональна мінімізація повноважень;

– наукова обґрунтованість і технічна реалізація;

– обов'язковість контролю;

– превентивний характер проведення заходів інформаційної безпеки щодо заходів інших видів безпеки.

Сучасні керівники підприємств у сфері економіки та бізнесу відчувають дефіцит спеціальної літератури з питань забезпечення інформаційної безпеки, що виступає як важлива складова загальної системи економічної безпеки господарюючого суб’єкта.

Вітчизняні системи інформаційної безпеки мають свої недоліки, обумовлені кількома причинами. По-перше, інформація, як цінний ресурс, легко копіюється, модернізується або знищується, що створює виклики для забезпечення її безпеки. По-друге, широкомасштабний розвиток обчислювальної техніки та телекомунікаційних систем призводить до складнощів у контролі та запобіганні несанкціонованого доступу до інформації, особливо при переході до безпаперової технології та розширенні кола користувачів.

Основні завдання інформаційної безпеки включають в себе виявлення, оцінку та запобігання загрозам для інформаційних систем і ресурсів. Також важливо забезпечувати захист прав юридичних і фізичних осіб на

інтелектуальну власність, а також ефективно керувати збором, нагромадженням та використанням інформації. Захист державної, службової, комерційної і особистої таємниці також є важливою складовою інформаційної безпеки.

1.2. Зовнішні та внутрішні загрози інформаційної безпеки підприємства

Під час глобальної цифровізації процесів, пов'язаних з веденням бізнесу та застосуванням у багатьох компаніях організації роботи персоналу у віддаленому режимі, збереження конфіденційної інформації підприємства почало займати пріоритетне місце в галузі прогнозування та запобігання потенційним загрозам та ризикам. Така тенденція призводить до збільшення навантаження на служби інформаційної безпеки на підприємстві, що, у свою чергу, змушує керівників модифікувати потужності з моніторингу, контролю, зберігання стратегічно важливої конфіденційної інформації шляхом придбання нового програмного забезпечення, пошуку компетентних фахівців в галузі інформаційної безпеки, не зацікавлених у створенні каналів витоків даних, що забезпечується лише на рівні кадрової безпеки організації [10].

Інформаційна безпека як один з невід'ємних системних компонентів економічної безпеки підприємства включає наступні заходи:

складання керівництвом локальної документації в галузі інформаційної безпеки для позначення меж секретності даних, що підлягають охороні від зловмисників;

створення рівнів доступу до інформаційної бази, сортування видів документації, що захищається за даними рівнями, визначення кола осіб, які входять до того чи іншого рівня доступу до баз даних;

оснащення організації економічно обґрунтованою системою програмного забезпечення, фізичними заходами запобігання створенню каналів витоків даних;

проведення роботи зі складом співробітників з питань забезпечення захисту конфіденційних ресурсів;

контроль документообігу під час укладання договорів співробітництва з контрагентами (постачальники, підрядники, кредитні організації);

зміна рівня секретності даних на більш високий або нижчий.

Отже, будь-яка зовнішня загроза впливає на інформаційну безпеку компанії, знижуючи її стійкість та можливість подальшого функціонування у цифровому середовищі. Однак окрему групу загроз, що впливають на інформаційну безпеку підприємства, представляють внутрішні виклики, що впливають на загальну систему економічної безпеки компанії (табл. 1.2).

Таблиця 1.2

Внутрішні загрози, що впливають на інформаційну безпеку підприємства

№ з/п	Опис загроз інформаційної безпеки	Вплив на загальну систему економічної безпеки підприємства
1.	Кадрова загроза, витік інформації внаслідок дій співробітників	Зниження фінансових результатів, поява збитків, вихід з ринку
2.	Втрата інформації внаслідок недобросовісної роботи персоналу з організації захисту інформації	Доступність інноваційних розробок конкурентам, втрата нових ринків збуту
3.	Зниження захисного потенціалу програмного забезпечення та серверів в організації	Збільшення витрат організації, брак ресурсів
4.	Недостатнє фінансування інформаційної безпеки	Нестача капіталу, як наслідок відсутності коштів на розвиток організації, загроза банкрутства
5.	Низькі темпи оновлення захисних систем, невчасність поповнення банків даних новими загрозами	Втрата ресурсів, витік інформації
6.	Витік даних клієнтів	Втрата клієнтів, витрати на відновлення захисних даних

Загалом інформаційна безпека організації формується за допомогою забезпечення кадрової, фінансової, ресурсної та інформаційної складових. Інформаційна загроза має місце тоді, коли величина та ймовірність можливої

інформаційної шкоди більша від певного порогового значення, що вимагає вжиття заходів щодо його запобігання, захисту об'єкта безпеки. Загрози безпеки, цілісності та конфіденційності інформаційних ресурсів обмеженого доступу практично реалізуються через ризик утворення каналу несанкціонованого отримання (добування) кимось цінної інформації та документів. Цей канал є сукупністю незахищених або слабко захищених напрямів можливої втрати інформаційних ресурсів обмеженого доступу, які зловмисник використовує для отримання необхідних відомостей. Функціонування каналу несанкціонованого доступу до інформації обов'язково спричиняє втрату інформації, зникнення носія інформації.

Забезпечення інформаційної безпеки має починатися з виявлення суб'єктів відносин, пов'язаних із використанням інформаційних систем. Спектр їх інтересів може бути поділений на такі основні категорії: доступність (можливість за прийнятний час отримати необхідну інформаційну послугу), цілісність (актуальність та несуперечність інформації, її захищеність від руйнування та несанкціонованої зміни), конфіденційність (захист від несанкціонованого ознайомлення). Виходячи з вищевикладеного, у найбільш загальному вигляді інформаційна безпека може бути визначена як неможливість завдання шкоди властивостям об'єкта безпеки, що обумовлюються інформацією та інформаційною інфраструктурою.

До об'єктів інформаційної безпеки в організації відносять:

- інформаційні ресурси, що містять відомості, віднесені до комерційної таємниці, та конфіденційну інформацію, подану у вигляді інформаційних масивів та баз даних;

- засоби та системи інформатизації – засоби обчислювальної та організаційної техніки, мережі та системи, загальносистемне та прикладне програмне забезпечення, автоматизовані системи управління в організаціях, системи зв'язку та передачі даних, технічні засоби збору, реєстрації, передачі, обробки та відображення інформації.

Підприємець, проваджуючи свою діяльність, стикається з обов'язком обробки, зберігання, перетворення, передачі та ліквідації інформації. Якщо певна інформація має велике значення для підприємця, її необхідно захищати від недобросовісних осіб. Значущість визначається такими параметрами, як корисність, достовірність, своєчасність і релевантність. Під час захисту інформації важливо блокувати всі можливі шляхи витоку та забезпечити безпеку зберігання інформації на всіх носіях на підприємстві.

Зовнішні загрози інформаційної безпеки включають копіювання цінних документів, викрадення файлів, втрату флеш-карт, а також можливість втрати інформації під час передачі по Інтернету. Додаткові ризики включають пошкодження носіїв інформації, розголошення інформації конкурентам чи іншим країнам, викрадення інформації інсайдерами та переманювання персоналу на інші фірми.

Серед внутрішніх загроз популярні крадіжки, зараження вірусами та порушення файлів співробітниками компанії. Причини внутрішніх загроз включають психологічні аспекти, такі як невдоволеність відносинами між співробітниками, недостатня заробітна плата та конфлікти між персоналом і керівництвом. За даними психологів, близько 25% співробітників можуть розголошувати, продавати або передавати інформацію конкуруючим компаніям.

Захист інформації на підприємстві є вкрай важливим, і це повинно бути враховано при укладенні контрактів з працівниками, особливо тими, які займають керівницькі посади. Основна небезпека становить загроза інформації, яка зберігається в інформаційних системах підприємства, що включають програмне забезпечення, програми для виконання завдань, текстові редактори та бази даних. Для гарантування безпеки інформаційної системи необхідно надавати повноваження зареєстрованим користувачам, обмежуючи їхні можливості використання інформаційних технологій.

Виявлення, аналіз та оцінка ризиків інформаційної безпеки є ключовим етапом проектування систем інформаційної безпеки підприємства. Від того,

наскільки правильно будуть оцінені ризики, залежить і ефективність системи інформаційної безпеки підприємства в цілому.

1.3. Управління інформаційною безпекою підприємства

Аналізуючи вимоги щодо захисту інформації, розглянемо поняття обчислювального середовища, в якому проводиться обробка даних за допомогою обчислювальних програм. Дані і програми розташовуються на внутрішніх носіях, а операційне середовище представляє собою елементи обчислювального середовища, що перебувають в оперативній пам'яті комп'ютера.

Захист елементів обчислювального середовища суттєво зводиться до захисту даних і програм. Засоби захисту інформаційної системи включають заходи з захисту елементів обчислювального середовища і контролю елементів операційного середовища.

Захист елементів обчислювального середовища охоплює: захист даних; засоби власного захисту програм; захист процедур обробки інформації.

Контроль елементів операційного середовища включає: контроль зовнішніх компонент операційного середовища; контроль цілісності внутрішніх компонент операційного середовища; контроль семантики даних.

Захист інформації реалізується різними методами, такими як захист програм від читання та копіювання, забезпечення авторських прав на інформацію, контроль несанкціонованого доступу і запуску програм, а також самотестування і самовідновлення коду програми.

Питання авторських прав стає ключовим у відношенні захисту інтелектуальної власності, і розробники програм приділяють йому особливу увагу. Захист програм від копіювання реалізується через програмні засоби, використовуючи ідентифікацію користувача, обмеження кількості запусків програми, обмеження за часом або кількістю запусків.

У глобальному середовищі забезпечення інформаційної безпеки на підприємстві передбачає постійний контроль за джерелами можливих загроз, таких як антропогенні, технологічні та стихійні, та вимагає застосування різноманітних заходів захисту інформації (захист від читання та копіювання, захист авторських прав, обмеження доступу та запуску програм, самодіагностика тощо).

Розглянемо найпопулярніші у час методики управління ризиками інформаційної безпеки [2].

Метод CRAMM (CCTA Risk Analysis and Managment Method) та однойменний програмний продукт, що його реалізує, від компанії Insight Consulting Limited є потужним та універсальним інструментом проведення обстеження інформаційних систем та аналізу ризиків інформаційної безпеки. Даний метод використовується вже понад 30 років і за цей час набув популярності у всьому світі. Основним недоліком методу є те, що він не враховує супровідної документації, і ідентифікація ресурсів, що захищаються, проводиться без прив'язки до бізнес-процесів підприємства.

Зазначеного недоліку не позбавлена й методика FRAP (Facilitated Risk Analysis Process), яку пропонує компанія Peltier and Associates. У цій методиці визначення ресурсів, що захищаються проводиться з використанням опитувальних листів, вивчення документації на систему, використання інструментів автоматизованого аналізу (сканування) мереж. Ідентифікація ресурсів, що захищаються, проводиться також без прив'язки до бізнес-процесів підприємства.

Метод CORAS є методикою і програмним інструментом моделювання ризику. Програмний продукт, що реалізує методологію CORAS, розповсюджується безкоштовно. У методиці CORAS не передбачено періодичності проведення оцінки ризиків та актуалізації їх значень. CORAS не дозволяє оцінити ефективність інвестицій, вкладених у впровадження заходів безпеки. Так само, як і в вищерозглянутих методиках, CORAS не дає

можливості аналізу бізнес-процесів підприємства з метою виявлення ресурсів, що захищаються.

Розроблена компанією RiskWatch однойменна методика орієнтована кількісні способи оцінки ризиків. Розмір ризику визначається як математичне очікування втрат протягом року.

Ефект від запровадження засобів захисту кількісно розраховується за допомогою показника ROI (Return on Investment – повернення інвестицій). Цей метод доцільно використовуватиме проведення аналізу ризиків на програмно-технічному рівні захисту без урахування організаційних та адміністративних чинників.

Методика Microsoft Security Assessment Tool (MSAT), реалізована у відповідному програмному продукті від компанії Microsoft, використовує якісні оцінки ризиків інформаційної безпеки. Методика дозволяє оцінити ефективність інвестицій від впровадження засобів захисту інформаційних активів, але не дає можливості брати до уваги бізнес-процеси, що протікають у компанії, з метою ідентифікації об'єктів захисту.

Усе сказане вище дозволяє зробити висновок про те, що на сьогоднішній день не існує загальноприйнятої науково обґрунтованої методики виявлення ризиків інформаційної безпеки.

Приватні методики, що використовуються при проектуванні системи інформаційної безпеки підприємств і організацій, здебільшого спираються на емпіричні підходи в оцінці ризиків інформаційної безпеки, засновані на накопиченому компаніями-розробниками досвіді розробки систем управління ризиками інформаційної безпеки [7].

Вважається, що основним недоліком більшості робіт, в яких викладено вищеописані методики, є їхня орієнтація на емпіричний підхід, недостатня увага до можливостей, що виникають при використанні методів та засобів проектування інформаційних систем. До таких методів належить і методика структурно-функціонального аналізу, що спирається на застосуванні CASE1-технологій.

У табл. 1.3 представлені засоби захисту інформаційної безпеки.

Таблиця 1.3

Класифікація засобів захисту інформаційної безпеки

№ з/п	Тип засобів	Характеристика
1.	Організаційні	Законодавчі та локальні нормативні акти, що регламентують сферу інформаційної безпеки, а також дії щодо обслуговування інформаційної інфраструктури
2.	Програмні	Спеціалізоване програмне забезпечення для зберігання, обробки та безпечної передачі інформації
3.	Апаратні	Електронні, механічні пристрої, інтегровані в обладнання автоматизованої інформаційної системи, або працюють як автономна апаратура, що захищають від проникнення в інформаційну інфраструктуру
4.	Апаратно-програмні	Сукупність спеціального обладнання та програмного забезпечення, що використовуються для захисту даних

Окремо варто розглянути програмні засоби захисту інформаційної безпеки. У цю групу входять насамперед антивіруси, які знешкоджують віруси та відновлюють заражені файли та програмне обладнання. Також є хмарні антивіруси. Рішення DLP (Data Leak Prevention) дозволяють запобігти витоку інформації, порушення її конфіденційності. Криптографія часто використовується для шифрування даних, для запобігання крадіжкам та витоку інформації.

Проксі-сервери виступають посередником між користувачами або системами. Безумовно, надійним та ефективним засобом захисту є також VPN, що в перекладі означає «віртуальна приватна мережа», що дозволяє використовувати приватну мережу для передачі або отримання інформації.

Таким чином, що інформація є найважливішим ресурсом життя і стає ключовим елементом практично всіх систем соціального життя. У будь-якій галузі, чи то політична безпека, економічна безпека, екологічна безпека, громадська безпека, існує сполучний елемент, у ролі якого виступає інформаційна безпека. У своїй фінансово-господарській діяльності

підприємство безперервно стикається з різними видами інформації, що надходить - з відкритою офіційною, ймовірною (неофіційною) і з таємницею, отриманою через неформальні контакти [6].

Для забезпечення захисту внутрішньої інформації керівництвом вживаються різні заходи:

щодо припинення можливості виробничого шпигунства та витоку інформації;

зі збору інформації про можливих ініціаторів шпигунства;

з технічного захисту документів, приміщень, транспорту;

з іншої зовнішньої інформаційної діяльності.

Саме тому для підприємства одним із пріоритетних напрямів економічної безпеки стає створення надійної системи, що ефективно працює з інформацією та забезпечує нейтралізацію внутрішніх та зовнішніх загроз.

Крім того, інформаційна безпека сучасного комерційного підприємства забезпечується шляхом впровадження комплексу стратегічних заходів та технологічних рішень. Основні складові забезпечення інформаційної безпеки наведено в табл. 1.4.

Таблиця 1.4

Складові забезпечення інформаційної безпеки підприємства

№ з/п	Складова	Характеристика
1	2	3
1.	Кіберзахист	Використання сучасних програмних та технічних засобів для захисту від кіберзагроз, таких як віруси, шкідливі програми, фішинг, атаки на мережевий рівень тощо.
2.	Шифрування даних	Застосування шифрування для захисту конфіденційної інформації під час її передачі або зберігання. Це зменшує ризик несанкціонованого доступу.
3.	Управління доступом	Встановлення строгих правил та обмежень доступу до інформації, враховуючи рівні привілеїв для різних користувачів та використання систем аутентифікації.
4.	Безпека мережі	Захист мережевої інфраструктури від несанкціонованого доступу та атак, включаючи застосування мережевих брандмауерів, систем виявлення вторгнень тощо.

Закінчення табл. 1.4

1	2	3
5.	Системи виявлення та реагування на інциденти	Розробка та впровадження систем, які автоматично виявляють потенційні інциденти безпеки та забезпечують швидке реагування на них.
6.	Фізична безпека інфраструктури	Захист серверних приміщень, дата-центрів та іншої інфраструктури від несанкціонованого доступу, використання систем відеоспостереження та систем контролю доступу.
7.	Навчання та підвищення обізнаності персоналу	Проведення тренінгів та навчань для працівників щодо безпеки в інформаційному просторі, виявлення соціального інженерінгу та інших загроз.
8.	Резервне копіювання та відновлення даних	○ Розробка та виконання стратегій резервного копіювання, які дозволяють відновлювати важливу інформацію в разі втрати або пошкодження даних.
9.	Впровадження стандартів безпеки	Дотримання стандартів та нормативів безпеки, які встановлюються для конкретної галузі чи регіону
10.	Аудит та внутрішній контроль	Проведення регулярного аудиту безпекових процесів та внутрішнього контролю для виявлення слабких місць та удосконалення систем безпеки.

Всі ці запропоновані заходи узгоджено впроваджуються для створення комплексної системи інформаційної безпеки, що забезпечує ефективний захист комерційного підприємства.

Отже, забезпечення інформаційної безпеки в підприємницькій діяльності в Україні вимагає комплексного підходу та використання різноманітних механізмів. Основні з них включають:

- розробка та впровадження політик та стандартів безпеки, які повинні дотримуватися всі працівники підприємства. Це може включати політики щодо доступу до інформації, захисту від зловживань, шифрування даних та інші аспекти безпеки;
- навчання політиці забезпечення інформаційної безпеки для персоналу, яке є ключовим елементом. Працівники повинні бути ознайомлені з потенційними загрозами, методами захисту та правилами користування інформацією;
- використання сучасних технологій та програмних засобів таких як використання антивірусного програмного забезпечення, систем виявлення

вторгнень, фаєрволів та інших засобів дозволяє ефективно виявляти та запобігати інформаційним загрозам.

- створення системи резервного копіювання та відновлення дозволяє підприємству швидко відновити свою діяльність в разі інциденту.
- фізична безпека, яка передбачає, що захист фізичного доступу до обладнання та інфраструктури є також важливим аспектом. Це може включати контроль доступу, використання біометричних технологій та інші заходи;
- моніторинг та аудит безпеки, які дозволяють виявляти аномалії та потенційні загрози, а також забезпечують відповідність встановленим стандартам;
- взаємодія з іншими підприємствами та організаціями та обмін інформацією та досвідом з іншими підприємствами і організаціями може сприяти виявленню нових загроз та розробці більш ефективних стратегій інформаційної безпеки.

Ці механізми разом створюють комплексний підхід до забезпечення інформаційної безпеки підприємницької діяльності в Україні.

Висновки до розділу 1

Об'єктивна потреба у створенні системи інформаційної безпеки підприємства випливає з ряду конкретних факторів. Першим із цих чинників є зростання обсягу інформації, що використовується в діяльності підприємства. У контексті інформаційного суспільства, інформаційні технології широко застосовуються в виробництві, переходячи від традиційного паперового документообігу до цифрового формату. Швидкий розвиток цих технологій призводить до поширення використання комп'ютерних засобів та їх об'єднання в мережі, що значно полегшує завдання обробки, обміну та доступу до інформації для кожного суб'єкта підприємницької діяльності.

Захист інформації на підприємстві є надзвичайно важливим аспектом, що повинен бути врахований під час укладання контрактів з працівниками, особливо тими, які обіймають керівницькі посади. Основною загрозою є потенційна небезпека для інформації, яка знаходиться в інформаційних системах підприємства, включаючи програмне забезпечення, виконавчі програми, текстові редактори та бази даних. Для забезпечення безпеки інформаційної системи належить надавати повноваження зареєстрованим користувачам, обмежуючи їхні можливості використання інформаційних технологій. Виявлення, аналіз та оцінка ризиків інформаційної безпеки представляють собою критичний етап у проектуванні систем інформаційної безпеки підприємства. Від того, наскільки точно будуть визначені та оцінені ризики, залежить ефективність системи інформаційної безпеки підприємства в цілому.

Отже, в умовах динамічного бізнес-середовища інформаційна безпека стає необхідною складовою економічної безпеки підприємства, а забезпечення цієї безпеки визначає успішний перехід до моделі сталого розвитку як окремого суб'єкта господарювання, так і національної економіки в цілому.

РОЗДІЛ 2. АНАЛІЗ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ТОВ «ІНТЕРЕНЕРГО ІНЖИНІРИНГ»

2.1. Характеристика суб'єкта підприємницької діяльності

У 2005 році було засновано науково-виробниче підприємство «Інтеренерго». Відтоді вона будує «під ключ» промислові енергетичні об'єкти в різних галузях, таких як металургія, хімія, харчова промисловість. Протягом 16 років компанія використовує передові технології та найсучасніше обладнання для вирішення складних завдань будівництва та запуску промислових енергетичних об'єктів, таких як біогазові, газотурбінні та газопоршневі електростанції, тепломасляні системи та котли.

Команда фахівців підприємства може похвалитися комплексною структурою, яка включає кваліфікованих дизайнерів, експертів з монтажу, спеціалістів з налагодження та групу управління проектами. Завдяки цьому ми маємо змогу з високим професіоналізмом та якістю виконувати складні проекти під ключ при будівництві енергетичних об'єктів. Ми співпрацюємо з партнерами з різних країн, включаючи Австрію, Німеччину, Францію, Польщу, Італію, Ізраїль, Туреччину та Болгарію. Команда фахівців підприємства швидко стала провідною у будівництві промислових енергетичних об'єктів в Україні та за її межами. Про це свідчить наш широкий список рекомендацій, що охоплює різні регіони як усередині країни, так і за кордоном.

Статут підприємства. Підприємство ТОВ «ІНТЕРЕНЕРГО ІНЖИНІРИНГ» зареєстрована 25.01.2005 за юридичною адресою 61001, Харківська обл., місто Харків, вул. Плеханівська, будинок 20 А. Керівником організації є Ісаченко Дмитро Андрійович. Розмір статутного капіталу складає 1 315 895,00 грн. На момент останнього оновлення даних 25.09.2021 стан організації - не перебуває в процесі припинення.

Відомості про сферу діяльності, юридична адреса: 61001, Харківська обл., місто Харків, вулиця Плеханівська, будинок 20 А.

Сфери діяльності:

Основна:

- 33.20 Установлення та монтаж машин і устаткування.

Інші:

- 46.69 Оптова торгівля іншими машинами й устаткуванням;

- 71.12 Діяльність у сфері інжинірингу, геології та геодезії, надання послуг технічного консультування в цих сферах;

- 74.90 Інша професійна, наукова та технічна діяльність,не введені в інші угруповання;

- 33.14 Ремонт і технічне обслуговування електричного устаткування;

- 77.33 Надання в оренду офісних машин і устаткування, у тому числі комп'ютерів;

- 68.20 Надання в оренду й експлуатацію власного чи орендованого нерухомого майна.

Розглянемо структуру підприємства ТОВ «ІНТЕРЕНЕРГО ІНЖИНІРИНГ» (рис. 1.1). Аналізуючи організаційну структуру, зображену на рис. 2.1, стає очевидним, що вона дотримується лінійно-функціонального підходу, який пропонує переваги як лінійної, так і функціональної структур. Ця модель полегшує ефективне прийняття рішень і сприяє індивідуальній відповідальності керівників за досягнення бажаних результатів продуктивності.

Найвищий рівень управління ПАТ «НПП ІНТЕРЕНЕРГО» займає генеральний директор, який одночасно є власником компанії.

До його функцій відносяться:

- основний обов'язок генерального директора – формувати стратегію розвитку підприємства, визначати місію та цінності, на яких базуються діяльність компанії. Щоб успішно виконати це завдання, генеральний директор повинен

враховувати інструкції та вказівки, надані радою директорів, керівним органом, який має повну владу як над компанією;

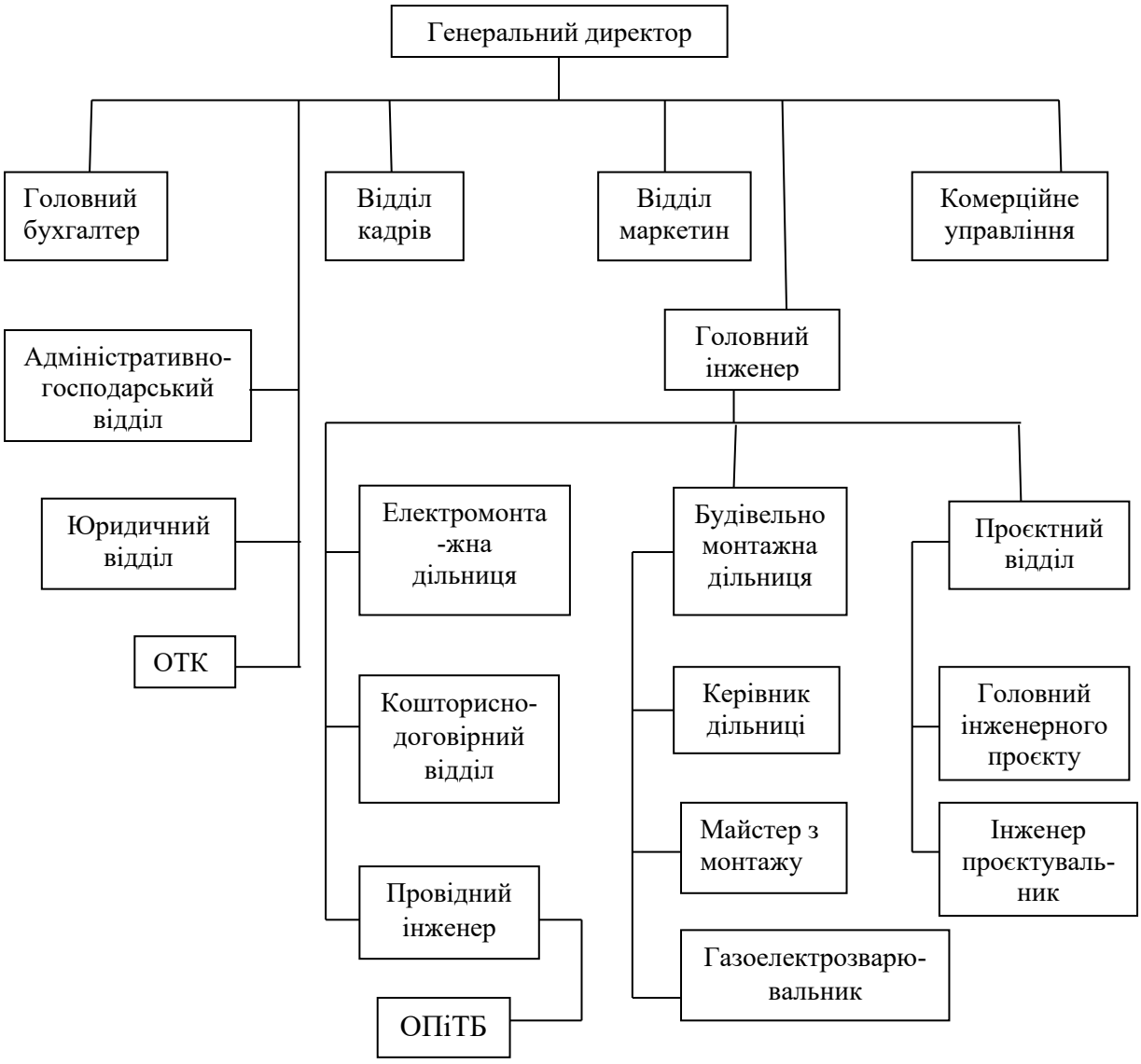

Рис. 2.1. Структура підприємства ТОВ «ІНТЕРЕНЕРГО ІНЖИНІРИНГ»

- генеральний менеджер зобов’язаний інформувати правління про важливі події, що відбуваються всередині та за межами організації, які потенційно можуть вплинути на дії підприємства;

- у деяких випадках допускається, щоб рішення щодо діяльності компанії приймалися без участі ради директорів;

- в рамках своїх обов'язків відповідає за пошук потенційних спонсорів та інвесторів, крім проведення переговорів з клієнтами. Це має вирішальне значення для просування обладнання і послуг компанії.

Юридичний відділ відповідає за виконання різноманітних функцій:

- налагоджують систематизований облік та збереження нормативно-правових актів;

- документальне оформлення прийнятих на підприємстві нормативно-правових актів щодо бухгалтерського обліку.

Відділ кадрів відповідає за виконання різних функцій:

- мінімізації плинності працівників;

- підвищення трудової дисципліни.

Функції проектного відділу:

- підвищує ступінь збалансованості програми робіт з ресурсним забезпеченням проекту;

- підвищується об’єктивність оцінки учасників проекту і т.п.

Функції маркетингового відділу:

- аналіз і прогнозування основних кон’юнктуроутворюючих факторів, потенційних ринків збуту, фінансовим станом потенційних покупців, платоспроможного попиту на продукцію підприємства;

- дослідження конкурентоспроможності виробленої продукції.

Функції кошторисного відділу:

- планування та організація виготовлення документації на капітальний та поточний ремонти приміщень, вентиляційного обладнання, електросистем, засобів зв'язку, сигналізації та інших інженерних систем;

- складає договорів та інших правових угод, пов'язаних з виконанням покладених на відділ обов'язків та їх подальше виконання у встановленому законодавством порядку.

Не дивлячись на те, що всі функціональні одиниці компанії виконують різні функції та підпорядковуються різним керівникам, вони пов’язані між собою та співпрацюють разом для досягнення цілей організації.

1) завдання організації з точки зору її основних послуг або товару, її основних ринків та основних технологій:

- підготовка ТЕО та розрахунок ефективності капіталовкладень;

- комплексне проектування;

- спорудження «Під ключ» енергетичних об’єктів;

- пусконалагоджувальні роботи і здача об’єкта в експлуатацію;

- сервісне обслуговування.

2) зовнішнє середовище по відношенню до організації, яке визначає основні робочі принципи організації.

Ключові фактори успіху організації знаходяться у зовнішньому середовищі.

Зовнішнє середовище – це перш за все ті організації, хто пов’язаний з бізнесом через цілі та завдання, які він виконує: постачальники, споживачі, акціонери, кредитори, конкуренти тощо, що впливає на його фундаментальні принципи:

- можливість вільно встановлювати ціни, дотримуючись правових норм;

- процес вибору постачальників і споживачів товарів (устаткування та ін.) є найважливішим аспектом обробної промисловості;

- прибутком, що залишився після законодавчо встановлених платежів, можна вільно розпоряджатися.

3) культура організації. Якого типу робочий клімат у колективі.

Культура організації має рівень «поверхневої». Про це свідчить фірмовий знак, місце на ринку, фірмовий одяг працівників, знаки фірми, свята підприємства, загальні обіди, різні засоби стимулювання працівників (наприклад, загальна поїздка на відпочинок на байдарках, похід у боулінг).

Причиною соціально-психологічного клімату є те, що:

- члени групи мають взаємні очікування та довіру один до одного;

- успіх команди значною мірою залежить від відсутності тиску з боку вищого керівництва на своїх підлеглих, що дозволяє членам команди мати свободу приймати важливі рішення для кращої роботи команди;

- щоб команда працювала належним чином, керівництву важливо утримуватися від тиску на підлеглих і визнавати їх право приймати ключові рішення для команди;

- наявність членів команди, які володіють достатніми знаннями про завдання та добре поінформовані про стан справ.

Місією підприємства ТОВ «Інтеренерго Інжиніринг» є сприяння економічному розвитку та добробуту підприємств, які обслуговуються компанією, шляхом надання громадянам і підприємствам якісних послуг комплексного будівництва та введення в експлуатацію об'єктів промислової енергетики: біогазові, газотурбінні та газопоршневі електростанції, , використання альтернативних видів енергії таким чином і в такому обсязі, які відповідають високим професійним і етичним стандартам, забезпечення справедливого і відповідного прибутку підприємства і справедливого відношення до співробітників компанії.

2.2. Оцінка ефективності використання трудових ресурсів підприємства

Під персоналом підприємства розуміється вся його робоча сила, яка охоплює всіх осіб у його штаті, незалежно від їхньої професійної чи кваліфікаційної категорії. Це включає експертів, робітників, техніків і керівників, а також персонал служби безпеки, стажерів і обслуговуючий персонал початкового рівня.

Стабільність робочої сили є вирішальним фактором у визначенні кадрового потенціалу підприємства, і часто вимірюється шляхом аналізу руху персоналу всередині компанії табл.2.1.

Таблиця 2.1

Характеристика руху кадрів

№ з/п	Показники	Звітній рік 2021	Поточний рік 2022	Відхилення (+,-) %
1	2	3	4	5
1	Середня облікова чисельність працівників, люд.	28	33	(+5), 85%
2	Прийнято працівників, люд.	2	4	(+2) 50%
3	Вибуло працівників, осіб, у тому числі: за власним бажанням; звільнено за порушення трудової дисципліни; звільнено за скороченням штатів	1	3	(+2), 33%
4	Коефіцієнт плинності кадрів	7.1%	12.1%	(+5), 59%
5	Коефіцієнт загального обігу кадрів	0,04	0,1	(+0,08), 33,3

На основі аналізу даних табл. 2.1 можна зробити такі висновки:

- підприємство має середню плинність кадрів, порівняно за попередні роки, сприяє своєчасному оновленню колективу;

- відсутність високої плинності кадрів говорить про те, немає проблем в середині компанії, які призводять до втрати прибутку через часту зміну персоналу;

- хороший клімат на підприємстві свідчить, що у поточному році приєдналося до колективу 5 осіб.

2.3. Оцінка конкурентоспроможності підприємства

Для оцінки іміджу господарського підприємства використовуються експертні оцінки. Комплексна оцінка іміджу підприємства передбачає оцінки діяльності підприємства конкурентами, що відображається в таблиці 2.2 діловий-рейтинг.

Таблиця 2.2

Діловий рейтинг ТОВ «ІНТЕРЕНЕРГО ІНЖИНІРИНГ»

Категорії	ТОВ «Інтеренерго Інжиніринг»	«ALBIZ»	«KTS»
Ціна	4	4	4
Якість	5	4,6	5
Асортимент	4,7	5	3,9
Послуги	5	4,8	3,4
У середньому	4,7	4,6	4,1

* Оцінка балів проводилася на основі опитування, за оцінкою експертів від 1 до 5 балів.
1 - дуже не подобається;
2 - не подобається;
3 - влаштовує;
4 - подобається;
5 - дуже подобається.

Отже, ми спостерігаємо, що у діловому рейтингу табл. 2.2 підприємство ТОВ «Інтеренерго Інжиніринг» займає 1 місце, на другому фірма «ALBIZ». А третя фірма «KTS» порівняно з нашим підприємством відстає по усіх показниках. Фірма «ALBIZ» обходить нас лише у категорії «асортимент», але все одно посідає 2 місце тому, що усі показники нижчі.

Після оцінки ділового рейтингу перейдемо до споживчого рейтингу табл.2.3.

Таблиця 2.3

Споживчий рейтинг ТОВ «ІНТЕРЕНЕРГО ІНЖИНІРИНГ»

Критерії	Оцінка
Якість товарів, що реалізуються	5
Широта асортименту товарів	3
Цінова політика	3,5
Режим роботи	4,5
Якість монтажних робіт	5
У середньому	4,2

* Оцінка балів проводилася на основі опитування, за оцінкою експертів від 1 до 5 балів.
1 – дуже не подобається;
2 – не подобається;
3 – влаштовує;
4 – подобається;
5 – дуже подобається.

Виходячи з табл. 2.3 можна побачити, що найвищу оцінку отримали 2 критерії, найнижчу серед усіх одна це свідчить про те, що підприємству слід звернути уваги на критерії у яких оцінка нижче найвищої, щоб вийти на новий рівень та мати більше перспектив у майбутньому.

Проаналізувавши складові внутрішнього середовища діяльності підприємства складемо структуру цілей (табл. 2.4).

Таблиця 2.4

Структура цілей

Основні бізнес-процеси підприємства	Короткострокові цілі (до 1 року)	Середньострокові цілі (від 1 року до 3 років).	Довгострокові цілі (від 3 до 5 років).
1	2	3	4
Виробництво (Послуги)	Збільшення виготовлення продукції.	Перевірка їх виконання, підвищення технічної кваліфікації підприємства та рівня виробництва організації.	Збільшення виробництва на 15%.
Персонал	Підвищення кваліфікації працівників та якості робочих місць тощо.	Підвищуючи ступінь орієнтації внутрішніх клієнтів компанії, співробітники будуть більш мотивовані та брати участь у вирішенні проблем компанії.	Підвищення ступеня клієнтоорієнтованості компанії та вдосконалення технологій.
Фінанси	Збільшення обсягів продажів з кожним роком.	Забезпечення виконання цілей всіх функціональних областей.	Забезпечення стабільного щорічного зростання доходу.

Джерелом інформації є матеріали, отримані в процесі проходження переддипломної практики.

2.4. Аназіз зовнішнього середовища підприємства

Проведемо аналіз зовнішнього середовища підприємства, спочатку роздивимося торгову силу покупця за допомогою табл. 2.5.

Таблиця 2.5

Характеристика сили покупця

Характеристика	Значення
Рівень інформованості покупця	Високий
Чутливість до ціни, до засобів стимулювання	Високий
Наявність відповідних вимог до якості товару	Має міжнародні стандарти
Орієнтація на відповідну торгову марку	Добра
Періодичність закупівель	Від пів року до року
Обсяг середньої покупки	-
Фінансовий стан	Стабільний
Можливість вибору продавця	Завжди
Співвідношення між ступенем залежності продавця від покупця та ступенем залежності покупця від продавця	Позитивне

Як ми можемо побачити з табл. 2.5 значення сили покупця є ваговим для підприємства, а також воно на протязі багатьох років випускає когенераційні системи, які відповідають міжнародним стандартам так, як це впливає на кількість продажу в цілому.

Наступним кроком проаналізуємо діяльність конкурентів у табл. 2.6.

Таблиця 2.6

Оцінка діяльності конкурентів підприємства

Назва фірм		ТОВ «Інтеренерго Інжиніринг»	«ALBIZ»	«KTS»
№	Показники	Бали		
		1	2	3
1	Доля ринку	2	2	3
2	Рентабельність обігу	1	2	3
3	Рентабельність капіталу	1	2	2
4	Частка власних оборотних коштів	2	1	2
5	Рівень ціни домінуючого товару	2	2	2
6	Широта асортименту	3	3	3
7	Якість товару	3	2	2
8	Система збуту	3	1	2
9	Рівень сервісу	3	2	2
10	Система управління	3	2	2
	Середній бал	2,3	1,9	2,3

*Шкала оцінювання
1- низький рівень
2-середній рівень
3 високий рівень

Зробивши аналіз оцінки діяльності конкурента у табл. 2.6 можна зробити висновок, що досліджуване підприємство та фірма «KTS» знаходяться на одному рівні, щоб випередити конкурента потрібно підвищити усі показники, які мають 1 и 2 бали до максимальної оцінки 3.

Після аналізу зовнішнього та внутрішнього середовища фірми складемо перелік фактичних сильних і слабких сторін досліджуваного підприємства, щоб краще про нього дізнатися надамо SWOT – матрицю у табл. 2.7.

Таблиця 2.7

SWOT - матриця підприємства ТОВ «Інтеренерго Інжиніринг»

Сильні сторони	Можливості
1	2
Протягом 16 років компанія використовує передові технології та найсучасніше обладнання для вирішення складних завдань будівництва	Збільшення клієнтури
Сучасне високотехнологічне обладнання	Стабілізація обсягу замовлень
Кваліфіковані експерти з монтажу, спеціалістів з налагодження та групу управління проектами	Зниження темпів інфляції
Співпрацює з партнерами з різних країн, включаючи Австрію, Німеччину, Францію, Польщу, Італію, Ізраїль, Туреччину та Болгарію.	Залучення інвесторів різних країн
Використання інноваційих технологій	Партнерство з банківською сферою для реалізації будівельних і фінансових проектів
Має власний сайт	
Достатній рівень виробничих потужностей для виконання наявної кількості замовлень	
Хороша репутація фірми	

Закінчення табл. 2.7

1	2
Слабкі	Загрози
Зменшення рентабельності, бо підприємство займається будівництвом великих об’єктів, які довго реалізуються та цикл виробництва становить рік, навіть і більше	Збільшення кількості активних конкурентів
Високі витрати	Несприятливі погодні умови додатково ускладнюють умови праці, погіршують продуктивність праці та сприяють скороченню чисельності працівників
Зменшення обсягів надання послуг	Виникнення труднощів при укладанні договорів із постачальниками та споживачами
Малий асортимент товарів	Здорожання ресурсів для виробництва
Досить висока цінова політика	Зростання рівня вимог покупців і постачальників

Заходи щодо покращення слабких сторін та загроз для підприємства:

1) допомога при експлуатації побудованих об’єктів, забезпечення витратними матеріалами та запасними частинами під час після їх продажного обслуговування;

Тобто фахівці з сервісу ще деякий час після введення в експлуатацію збудованого об’єкту можуть працювати на ньому, доки замовник не сформує свою бригаду. Підприємство отримає дохід від цієї діяльності та покращить фінансові результати.

2) закупівля спеціальних станків (машини,механізми) для виготовлення металоконструкцій власними силами;

3) розширення асортименту завезення устаткування (не тільки когенераційні установки, а й теплові пункти, холодильні установки, трубопровідні арматура) та його комплектуючих з країн ЄС власними силами, що робить дешевшим кінцевий продукт, а значить сприяє росту конкурентоспроможності підприємства та надає можливості отримання

контрактів за рахунок нижчої ціни та збільшення обсягів виробництва у довгостроковій перспективі;

4) професійне навчання проектного/сервісного персоналу для можливості активізації інноваційної діяльності персоналу/ ремонту змонтованого устаткування та систем тощо;

5) оволодіння новітніми технологіями тепло та енергозабезпечення промислових підприємств, як необхідна умова розширення та диверсифікації діяльності, задля забезпечення задоволення постійно змінних вимог споживачів та науково-технічного прогресу. Це сприятиме не втраті попиту на свою продукцію, а можливо і зростанню обсягів виробництва та продажу.

Тепер детальніше ознайомимося з тим, яку продукцію пропонує підприємство.

Розглянемо на прикладі когенераційної установки.

Когенераційна установка працює за простим принципом: газоподібне паливо, таке як природний газ, біогаз або шахтний метан, подається в газопоршневий двигун, де воно спалюється для приводу поршневої групи.

Енергія, вироблена машиною, передається через вал до генератора, який потім перетворює її в електричну енергію.

На теплоелектростанції при виробленні електроенергії одночасно виділяється і тепло. Це тепло виходить від вихлопних газів, масла та охолоджуючої рідини, яка охолоджує двигун. Для видалення цього тепла використовується серія теплообмінників для нагрівання водопровідної води, а випускний теплообмінник використовується для виробництва пари та нагріву водопровідної води. В результаті когенерація максимально використовує теплову енергію. Вироблену електроенергію можна використовувати для власних потреб або продавати в централізовану мережу за комерційними тарифами.

При впровадженні когенераційних установок у різних галузях промисловості слід враховувати кілька аспектів:

1) Стала можливою утилізація великої кількості органічних відходів із додатковою перевагою виробництва електроенергії за допомогою сучасних методів збору біопалива. Біогазова теплоелектростанція ефективно вирішує цю проблему і має можливість працювати навіть на сирих паливних сумішах;

2) Технічний цикл підприємства проходить злагоджено та безперебійно завдяки зусиллям ТЕЦ, яка є надійним джерелом тепла, охолодження та електроенергії;

3) Газопоршневі агрегати MWM є високорентабельними, з максимальним споживанням природного газу від 0,24 до 0,25 м3/кВт·год і використанням моторного масла лише від 0,15 до 0,3 г на кожен 1 кВт·год виробленої електроенергії. Крім того, ці установки можуть генерувати від 427 до 4160 кВт безкоштовної теплової енергії у вигляді гарячої води з температурою від 90 до 110 градусів цельсія, а також пари для виробничих потреб за допомогою котлів-утилізаторів [35].

Теплові електростанції використовує широкий спектр об’єктів, таких як житлові райони, аеропорти, лікарні, муніципалітети, а також промислові та сільськогосподарські підприємства. Ці електростанції служать для підвищення надійності електропостачання при одночасному зниженні витрат, пов’язаних із закупівлею електроенергії у зовнішніх постачальників та сплатою плати за її транспортування та розподіл. В Україні успішно впроваджується когенерація, завдяки якій споживання енергоресурсів скорочується до 40% порівняно із закупівлею електроенергії із загальної мережі [34].

Висновок: проаналізувавши SWOT аналіз підприємства, рух кадрів, діловий рейтинг за певними критеріями оцінок ми бачимо, що фірма хоча і знаходиться на перших місцях, але конкуренти теж її наздоганяють, тому треба зосередитись на досконалості своїх можливостей у майбутньому.

2.5. Оцінка й аналіз фінансових ресурсів підприємства

Проведемо аналіз фінансово-економічного стану ТОВ «Інтеренерго Інжиніринг» та майна підприємства, розподілимо однорідні за змістом статті балансу, визначимо структуру та склад майна компанії (табл. 2.8).

Таблиця 2.8

Аналіз складу та структури майна ТОВ «Інтеренерго Інжиніринг», тис. грн. за 2020-2022 роки

Показник	Роки			2021/2020		2022/2021	
	2020	2021	2022	+/-	%	+/-	%
Усього майна	86 965	32 273	154 609	-54 692	37,11	122 336	479,07
Необоротні активи	193	149	131	-44	77,20	-18	-12,08
Оборотні активи	86 772	32 124	154478	-54 648	37,02	122 354	380,90
Запаси	8 619	4 279	26 525	-4 340	49,65	22 246	519,89
Дебіторська заборгованість	58143	6092	80818	-52 051	10,48	74 726	1226,63
Кошти та їх еквіваленти	6	21 256	37 746	21 250	354266,67	16 490	77,58

З табл. 2.8 можна побачити, що вартість усього майна підприємства у 2021р. порівняно з 2020 роком зменшилась на 55 млн. грн, з 87 млн. грн. до 32 млн. грн, при цьому темп приросту є 37,11%. Тепер можна поглянути на 2022 рік де відбулось збільшення вартості майна ТОВ «Інтеренерго Інжиніринг» порівняно з 2021 роком, на 122 млн. грн, з 32 млн. грн. до 155 млн. грн, причиною цього може бути те, що з кожним роком збільшувався показник кошти та їх еквіваленти, адже вони свідчать про поліпшення фінансового стану підприємства.

Обсяги оборотних активів підприємства у 2021 році зменшилися порівняно з 2020 роком, так як у 2020р. вони становили 87 млн. грн, а в 2021 році становили 32 млн. грн. (тобто зменшилися на 37,02%). Якщо поглянути на 2022 рік, то можна спостерігати доволі велике збільшення порівняно з 2021 роком, а саме з 32 млн. грн. до 154 млн. грн.

Тепер перейдемо до необоротних активів. З 2020 року до 2022 можна спостерігати лише зниження активів.

Також можна добре помітити, що показник коштів та їх еквівалентів значною мірою збільшувався з кожним роком. Якщо порівняти 2020 рік й 2021р. то можна побачити, що з 6 тис. грн. став 21 млн. грн. Стосовно 2022 року, то порівняно з 2021 показник виріс до 38 тис. грн (на 77,58%).

Проаналізуємо показники майнового стану ТОВ «Інтеренерго Інжиніринг», використовуючи наступні формули та занесемо отримані результати до табл. 2.9.

Таблиця 2.9

Аналіз показників майнового стану ТОВ «Інтеренерго Інжиніринг» за 2020-2022 роки

Показник	Роки			2021/2020		2022/2021	
	2020	2021	2022	+/-	%	+/-	%
1	2	3	4	5	6	7	8
Вартість всього майна тис. грн.	86 965	32 273	154 609	-54 692	37,11	122 336	47,90
Вартість власних коштів підприємства тис. грн.	2783	3623	4037	840	130,18	414	111,43
Вартість власних оборотних коштів (робочий капітал) тис. грн.	-2976	3474	3906	6450	-116,73	432	112,44
Коефіцієнт зносу	0,80	0,85	0,87	0,05	106,30	0,02	102,35
Коефіцієнт придатності	0,20	0,15	0,13	-0,05	75,00	-0,02	86,67

Виходячи з табл. 2.9 можна зробити висновок стосовно показника вартості всього майна про який ми вже використовували у табл. 2.8 та розписували про нього у висновку під табл. 2.8 тому не будемо про нього говорити. Тому перейдемо до вартості власних коштів підприємства, тут можна побачити, що вона повинна з кожним роком збільшуватися і ми можемо спостерігати за цим. Розглянемо детальніше у 2021порівняно з 2020 роком він збільшився на 840 тис. грн. з 2783 млн. грн. до 3623 млн. грн., при цьому темп

приросту складає 130,18%. Аналогічна ситуація відбувається між 2022 та 2021 роком де збільшення відбувається на 414 тис. грн., з 3623 млн. грн. до 4 млн. грн.

Вартість власних оборотних коштів (робочий капітал). Саме тут потрібно відмітити, що цей показник є основним на підприємстві обігових коштів, який має здатність безперешкодно вести повсякденну господарську діяльність без залучення кредиту. Таким чином видно, що цей показник також збільшнаглядується з кожним роком якщо взяти загалом, то з 2020 року до 2022 року він зріс на 9 млн. грн. з – 3 млн. грн. до 4 млн. грн.

Коефіцієнт зносу. З кожним роком показник тільки збільшується, про те це не є добрим для даного підприємства, так як свідчить погіршення стану матеріально-технічної його бази. Коефіцієнт придатності. За нормою він повинен бути більше 0,5 і ми сміливо можемо сказати, що значення з кожним стають все менше, проте вони не перейшли границю норми. Наступним кроком буде проведено аналіз фінансової стійкості підприємства, наведений у табл. 2.10.

Таблиця 2.10

Аналіз фінансової стійкості ТОВ «Інтеренерго Інжиніринг» за 2020-2022 рр

Показник	Роки			2021/2020		2022/2021		
	2020	2021	2022	+/-	%	+/-	%	Динаміка значень
1	2	3	4	5	6	7	8	9
1) коефіцієнт автономії	0,03	0,11	0,03	0,08	350,80	-0,09	23,3	Більше 0,5
2) коефіцієнт маневреності власних коштів	1,07	0,96	0,92	-0,11	89,67	-0,04	96,25	Більше 0,1
3) коефіцієнт концентрації залученого капіталу	1,03	0,89	0,97	-0,14	86,02	0,09	109,70	Менше 0,5
4) показник заборгованості кредиторам	0,98	0,79	0,61	-0,18	81,25	-0,19	76,70	Якомога менший
5) коефіцієнт покриття запасів (Кпз)	-0,11	-0,70	0,13	-0,58	620,75	0,83	-18,83	0,6-0,8

Отже, за результатами аналізу, наведеного в табл. 2.10, можна зробити наступні висновки:

1) подивившись візуально на цей показник без динаміки одразу помітно, що найкраще значення було в 2021р., але в 2020 та 2022 роках показники однакові й менше норми;

2) стосовно цього показника можна помітити, що з кожним роком він тільки зменшувався і становився менше одиниці, дивлячись на норму, то підприємство має позитивне значення;

3) якщо подивитись на цей показник, то можна зрозуміти, що 2021 році порівняно з 2020р. він став менше на 0,14 це є дуже добрим. Проте у 2022 році порівняно з 2021р. він знову зріс на 0,09 і його значення дорівнює 1, але такий показник свідчить про те, що на підприємстві більшу частину займають борги, ніж активи;

4) у 2021р. порівняно з 2020 роком показник зменшився на 0,18 (у відсотках на 81,25), аналогічно й у 2022р. порівняно з 2021 р. відбулося зменшення. Це є дуже добрим, адже чим нижчий показник тим краще.

Проаналізуємо показники прибутковості підприємства, які наведено в табл. 2.11.

Таблиця 2.11

Аналіз прибутковості ТОВ «Інтеренерго Інжиніринг» за 2020-2022 роки

Показник	Роки			2021/2020	2022/2021	
	2020	2021	2022	+/-	+/-	Динаміка значень
1	2	3	4	5	6	7
1) рентабельність продаж %	0,25	11,42	0,26	11,18	-11,16	Більше 20%
2) рентабельність операційної діяльності %	0,24	11,51	0,26	11,27	-11,26	Більше 20%
3) рентабельність діяльності до оподаткування %	0,19	23,57	0,33	23,38	-23,24	Більше 20%
4) рентабельність власного капіталу %	5,60	200	10,80	194,38	-189,19	Більше 16%

За результатами розрахунків, наведених в табл. 2.11 можна зробити такі висновки, що найбільше значення показників фіксується в 2021 році, самі найменші можна помітити в 2020 році. Проте тільки третій та четвертий показники у 2021 році мають значення більше 20 та 16%. Господарська операційна діяльність підприємства характеризує малу прибутковість підприємства у 2022 році, через великий спад значень усіх показників (особливо четвертий показник) порівняно з 2021 роком. Проте, тільки четвертий показник у 2022 році мав найбільше значення серед інших показників цього року.

Далі проаналізуємо оцінку ділової активності підприємства (табл.2.12).

Таблиця 2.12

Ділова активність ТОВ «Інтеренерго Інжиніринг» за 2020-2022 роки

Показник	Роки			2021/2020	2022/2021	
	2020	2021	2022	+/-	+/-	Динаміка значень
1	2	3	4	5	6	7
1) загальна оборотність капіталу	0,7	2,1	1,2	1,3	-0,8	збільшення
2) оборотність запасів	2,3	15,6	7,2	13,3	-8,3	збільшення
3) оборотність дебіторської заборгованості	1,1	10,9	2,4	9,8	-8,6	збільшення
4) середній строк обороту дебіторської заборгованості (к-ть днів)	322	33	152	-288,7	118,8	Зменшення
5) оборотність кредиторської заборгованості	0,8	2,8	2,0	2,0	-0,7	Збільшення
6) середній строк обороту кредиторської заборгованості к-ть днів)	468	130	176	-338,1	46,1	Зменшення
7) фондовіддача тис. грн.	352,8	389,4	1370,0	36,6	980,6	Збільшення
8) оборотність власного капіталу	23,4	18,4	47,5	-5,0	29,1	Збільшення

За результатами аназу показників табл. 2.12, необхідно звернути увагу на 3 головні показника, а саме на: загальну оборотність капіталу, фондовіддачу необоротних активів та оборотність власного капіталу:

1) загальна оборотність капіталу в 2021 році порівнняо з 2020р. зросла на 1,3, проте вона змнешилась в 2022 році майже в 2 рази. Тому найбільше зростання можна побачити лише в 2021 році, також добре те, що показник у 2022 році не впав нижче значення у 2020 році.

7) в період дослідження протягом 2020-2022 роках спостерігається підвищення ефективності використання основних засобів підприємства. Якщо порівняти 2020 та 2022 роки, то фондовіддача зросла в 4 рази порівняно з 2020 роком рис. 2.2.

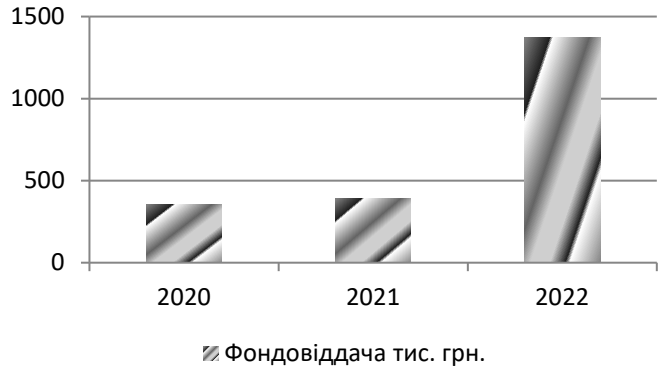

Рис. 2.2. Динаміка фондовіддачі за 2020-2022 роки

8) відносно цього показника помітно зменшення в 2021 році порівняно з 2020 роком, було 23,4 а стало 18,4. Проте значення цього показника в 2022 році значно збільшилось при тому, що в 2021 був 18,4 став 47,5. Коли ми побачили високе значення показника то можна зрозуміти, що власник підприємства ефективно використовує свій капітал. Щоб краще зрозуміти динаміку подивимося на рис. 2.3.

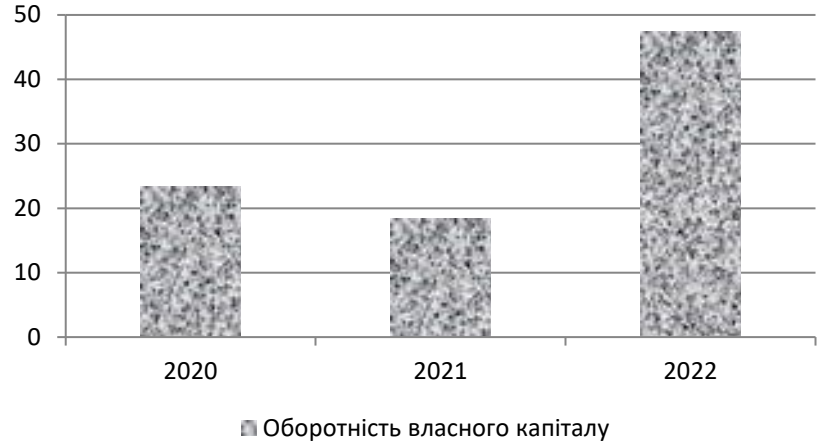

Рис. 2.3. Динаміка оборотності власного капіталу за 2020-2022 роки

Проаналізуємо динаміку доходів та витрат підприємства табл. 2.13.

Таблиця 2.13

Динаміка доходів тис. грн. ТОВ «Інтеренерго Інжиніринг» за 2020-2022 роки

Показник	Роки			2021/2020	2022/2021
	2020	2021	2022	+/-	+/-
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	65084	66579	191800	1495	125221
Інші операційні доходи	1027	7088	5525	6061	-1563
Всього доходів	66111	73667	197325	7556	123658

З отриманих даних в табл. 2.13 можна зрозуміти, що підприємство значно поліпшило результат показника як чистий дохід від реалізації продукції протягом 2020 по 2022 роки. Якщо подивитись, то з 2020р. до 2021 року він не значною мірою збільшився, але у 2022 році він збільшився до 192 млн. грн. (майже у 3 рази порівняно з 2021 та 2020 роках на рис. 2.4). На це могло вплинути збільшення ціни на обслуговування промислових енергетичних об'єктів, значне прискорення реалізації цих об'єктів тощо.

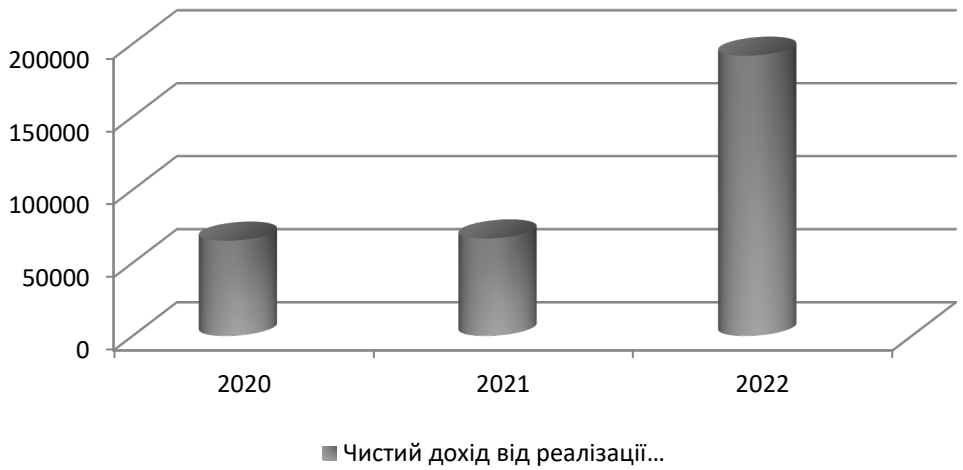

Рис. 2.4. Динаміка чистого доходу від реалізації продукції за 2020-2022 роки

Стосовно інших операційних доходів у 2021 зросли на 6 тис. грн. з 1 млн. грн. до 7 млн. грн., при цьому збільшилися вони в 6 разів. У 2022 році спостерігається спад на 1,5 млн. грн. порівняно з 2021.

Тепер розрахуємо динаміку витрат підприємства (табл. 2.14).

Таблиця 2.14

Динаміка витрат тис. грн. ТОВ «Інтеренерго Інжиніринг» за 2020-2022 роки

Показник	Роки			2021/2020	2022/2021
	2020	2021	2022	+/-	+/-
Собівартість продукції (товарів, робіт, послуг)	55725	61857	188396	6132	126539
Адміністративні витрати	1344	3027	2463	1683	-564
Інші операційні витрати	8881	1447	5961	-7434	4514
Всього витрат	65950	66331	196820	381	130489

З табл. 2.14 дуже помітним показником виступає собівартість продукції яка дуже зросла за 3 роки, при тому, що в 2020 вона становила 56 млн. грн. а у 2022р. зросла до 188 млн. грн. (у 3 рази більше ніж у 2020). На це вплинули такі фактори як: стан економік країни в цілому, валютний курс, подорожчання усіх матеріалів на будівництво, зміна асортименту об’єктів будівництва.

Також для більшого наочного вигляду показників адміністративних витрат та інших операційних витрат наведено на рис.2.5.

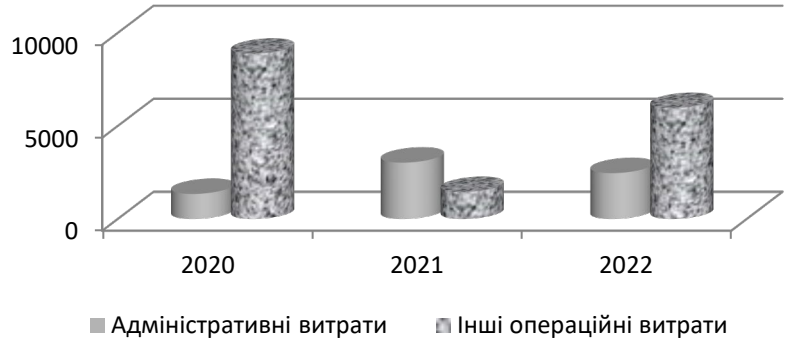

Рис. 2.5. Динаміка адміністративних витрат та інших операційних витрат за 2020-2022 роки

Найвище значення адміністративних витрат було зафіксовано у 2021 році, проте у 2022 р., він зменшився з 3 тис. грн. до 2,5 млн. грн. це теж впливає на позитивну динаміку.

Операційні витрати найбільше значення набули у 2020 році, проте вони дуже зменшилися у 2021р., з 9 млн. грн. до 1,5 млн. грн., але почали набирати обертів і збільшилися до 6 тис. грн. у 2022 році.

Провівши детальний аналіз фінансового стану ТОВ «Інтеренерго Інжиніринг» можемо зробити висновок, що підприємство хоч і має декілька показників з негативною динамікою, про те воно намагається з кожним роком мінімізувати свої слабкі сторони, продовжуючи активно розвиватися у своїй галузі будівництва енергетичних об’єктів (когенераційних установок, газотурбінних і газопоршневих електростанцій, біогазових заводів тощо).

2.6. Аналіз управління фінансовими ресурсами

Проаналізуємо показники ефективності використання фінансових ресурсів підприємства, а саме показники ліквідності та платоспроможності підприємства, ймовірність банкрутства. Для аналізу ліквідності балансу підприємства згрупуємо кошти за ступеню їх ліквідності табл. 2.15.

Таблиця 2.15

Групування активів підприємства ТОВ «Інтеренерго Інжиніринг» за 2020-2022 роки

Група	Умовне позначення	Роки		
		2020	2021	2022
1	2	3	4	5
Абсолютно-ліквідні активи	А1	6	21256	37746
Швидко-ліквідні активи	А2	58143	6092	80818
Повільно-ліквідні	А3	28872	4776	35914
Важко-ліквідні	А4	193	149	131

Тепер побудуємо таблицю 2.16 де будемо бачити групування зобов'язань підприємства за строками їх погашення.

Таблиця 2.16

Групування пасивів підприємства ТОВ «Інтеренерго Інжиніринг» за 2020-2022 роки

Група	Умовне позначення	Роки		
		2020	2021	2022
1	2	3	4	5
Найбільш термінові	П1	89748	28723	150619
Короткострокові	П2	0	0	0
Довгострокові	П3	0	0	0
Постійні (стійкі)	П4	-2783	3623	4037

Для проведення аналізу ліквідності балансу необхідно:

1) статті активу згрупувати за ступенем їхньої ліквідності і розмістити в порядку зменшення ліквідності:

- високоліквідні активи (А1);
- швидко ліквідні активи (А2);
- повільно ліквідні активи (А3);

- важко ліквідні активи (А4);

2) статті пасиву згрупувати за строками їхнього покашення і розмістити в порядку збільшення цих строків:

- найтерміновіші зобовязання (П1);

- короткострокові пасиви (П2);

- довгострокові пасиви (П3);

- постійні (стійкі) пасиви (П4);

3) порівняти суми в розрізі наведених груп за активом і пасивом балансу; баланс вважається ліквідним, якщо виконуються такі умови:

- А1≥П1;

- А2≥П2;

- А3≥П3;

- А4≥П4.

Після розрахунків в табл. 2.15 та 2.16 можна зробити співвідношення груп. А1≤ П1 впродовж 2020-2022 років, А2≥П2 та А3≥П3протягом досліджуваного періоду, якщо порівняти 2020 та 2021 рік то в 2020 було А4≥П4, але з 2021р., по 2022р., ситуація змінилася в інший бік А4≤ П4. Отже, як свідчить аналіз даних табл. 4.2, баланс досліджуваного підприємства з у 2020 році був не абсолютно ліквідним, оскільки не виконується перше співвідношення (А1≥П1). З 2021 по 2022 роки не виконувалися дві умови, а саме А1≤ П1 та А4≤ П4. Також помітно, що не виконується перша умова протягом досліджуваного періоду де абсолютно - ліквідні активи не покривають найбільш термінові зобов’язання.

Якщо брати до уваги перші три співвідношення з 2020 по 2022 рік можна помітити, що тут виконується 2 та 3, а саме А2≥П2 та А3≥П3, а перше ні так як А1≤ П1.

Тепер пропоную приділити більше уваги співвідношенню по роках 2021-2022 адже вони є більш актуальні ніж 2020-2021роки. Через те, що як ми вже проаналізували ці роки можна зробити висновок, що баланс не є ліквідним.

Підсумовуючи результати аналізованого періоду з цього випливає те, що ліквідність балансу відрізняється від абсолютної.

Після цього виконаємо аналіз відносних показників ліквідності у табл. 2.17.

Отже, з табл. 2.17 можна зробити такий висновок, що баланс ТОВ «Інтеренерго Інжиніринг» виявився ліквідний тому, що показники знаходяться в межах норми та намагається збільшувати свої активи з кожним роком задля покриття власних зобов'язань.

Таблиця 2.17

Аналіз відносних показників ліквідності ТОВ «Інтеренерго Інжиніринг» за 2020-2022 роки

Показник	Роки			2021/2020	2022/2021	
	2020	2021	2022	+/-	+/-	Динаміка значень
1) чистий оборотний капітал, тис. грн	-2976	3474	3906	6450	432	>0
2) коефіцієнт поточної ліквідності	0,97	1,12	1,03	0,15	-0,09	Зростання 1-2
3) коефіцієнт швидкої ліквідності	0,65	0,95	0,79	0,30	-0,16	Зростання 0,7-1,5 не більше 2
4) коефіцієнт абсолютної ліквідності	0,000067	0,74	0,25	0,74	-0,49	Зростання 0,2

Як можна помітити, самі високі показники можна зафіксувати у 2021 році, хоча чистий оборотний капітал збільшився у 2022 році на 432 тис. грн,, коли в інших показниках зменшився порівняно з 2021 роком. Для більшого розуміння щодо динаміки показників побудуємо графіки, зображені нижче на рис. 2.6.- 2.8:

помітні зміни відбулися з 2020 по 2021 рік коли підприємство покрило збиток та збільшилося з -3,4 млн. грн. до 4 тис. грн. рис.

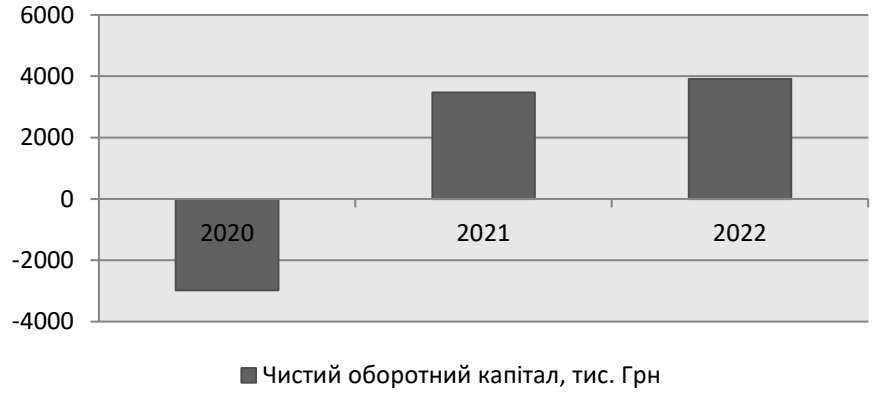

Рис. 2.6. Динаміка чистого оборотного капіталу, тис. грн. за 2020-2022 роки

стосовно коефіцієнта поточної ліквідності 2020 по 2021 спостерігається збільшення з цим пов’язано підвищення суми оборотних активів і зниження суми поточних зобов'язань, але в 2022 видно, що показник зменшився. Тепер перейдемо до коефіцієнта швидкої ліквідності, протягом цих років показник знаходяться в межах норми, не дивлячись, що в 2022 році відбулося зменшення. З цього виходить те, що на підприємстві досить оборотних коштів задля завчасного розрахунку з кредиторами.

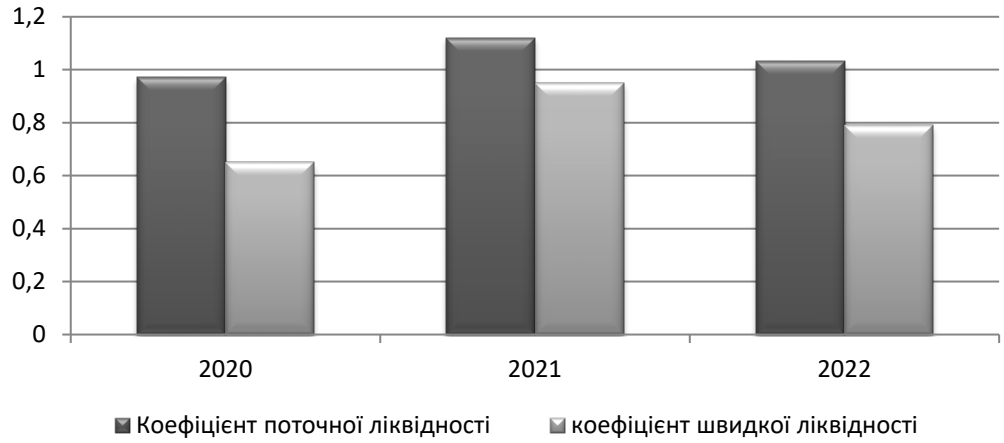

Рис. 2.7. Динаміка коефіцієнта поточної та швидкої ліквідності за 2020-2022 роки

аналізуючи цей коефіцієнт можна сказати, що в 2021 році він був дуже високим порівняно з 2020 та 2022 роком і це говорить про те, що підприємство

має неефективну стратегію використання фінансових ресурсів. Поглянувши на 2022 рік ми бачимо хороші зміни де відбулося покращення частини капіталу, яка використовувалася для непродуктивних активів рис. 2.8.

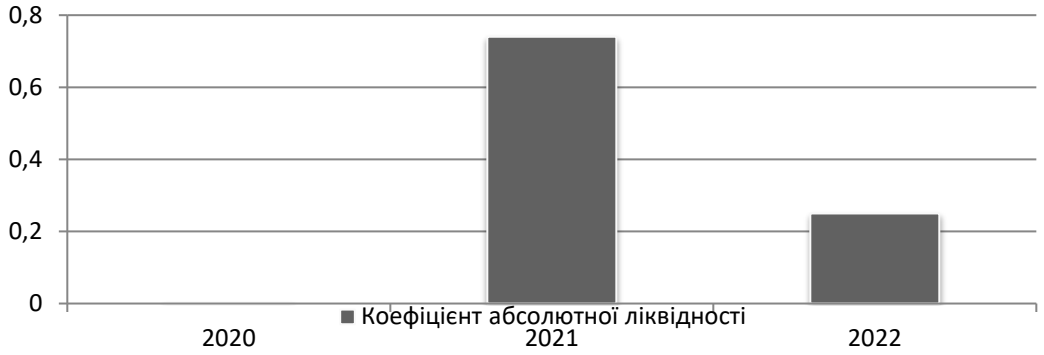

Рис. 2.8. Динаміка коефіцієнта абсолютної ліквідності за 2020-2022 роки

Далі необхідно визначити на якому рівні платоспроможності знаходиться підприємство, за допомогою табл. 2.18.

Таблиця 2.18

Критерії розподілу підприємств за рівнем платоспроможності

Критерії	Рівень платоспроможності підприємства	Характеристика
1	2	3
А1>П1+П2	Високий	Підприємство вирізняється значною ліквідністю та платоспроможністю, причому всі активи формуються переважно за рахунок власних коштів.
А1+А2>П1+П2		
А1+А2+А3>П1+П2		
А1+А2+А3+А4>П1+П2		
А1<П1+П2	Середній	Компанії не вистачає достатньо ліквідних ресурсів, які були б негайно доступні. Як правило, підприємства мають надійну ліквідність і можуть забезпечити своєчасне виконання зобов'язань щодо платежів.
А1+А2>П1+П2		
А1+А2+А3>П1+П2		
А1+А2+А3+А4>П1+П2		
А1<П1+П2	Помірний	Оборотний капітал компанії в основному складається з резервів, які були створені за рахунок позикових коштів. Очевидно, що підприємство неефективно використовує свої оборотні кошти, про що свідчить наявність великих запасів.
А1+А2<П1+П2		
А1+А2+А3>П1+П2		
А1+А2+А3+А4>П1+П2		

Закінчення табл. 2.18

1	2	3
А1<П1+П2	Низький	Оборотні активи підприємство створює виключно за рахунок короткострокових позикових коштів. Це призводить до того, що оборот підприємства базується не на власних, а виключно на позикових коштах. Крім того, частина поточного боргу компанії резервується для розвитку неліквідних активів.
А1+А2<П1+П2		
А1+А2+А3<П1+П2		
А1+А2+А3+А4>П1+П2		
А1<П1+П2	Підприємство перебуває на межі банкрутства	Якщо активи компанії не можуть покривати поточні зобов'язання, вона вважається банкрутом. Цей статус часто є результатом збиткової діяльності з непокритими збитками, які зменшують власний капітал компанії.
А1+А2<П1+П2		
А1+А2+А3<П1+П2		
А1+А2+А3+А4		

Щоб дізнатися його рівень потрібно зіставити табл. 2.15 і 2.16. та виконати розрахунок за роками табл. 2.19.

Таблиця 2.19

Значення показників за критеріями платоспроможності

за 2020-2022 роки

Роки		
2020	2021	2022
6 < 89748	21256 < 28723	37746 < 150619
58149 < 89748	27348 < 28723	118564 < 150619
87021 < 89748	32124 > 28723	154478 > 150619
87214 < 89748	32273 > 28723	154609 > 150619

З даної таблиці можна добре побачити, що підприємство в 2020році була жахлива ситуація, проте починаючи з 2021 року становище стало виходити на помірний рівень. Це може бути пов'язано з поліпшенням результатів його виробничо-господарської діяльності.

Водночас міцне фінансове становище залежить і від раціональної організації використання фінансових ресурсів. Таким чином, у ринковій економіці необхідно оцінювати не тільки активи та пасиви балансу, але також щоденно глибоко аналізувати стан і використання економічних активів.

Як і було зазначено вище, наступним кроком будемо розраховувати ймовірність банкрутства підприємства.

Для підтвердження висновків щодо ефективності діяльності підприємства розрахуємо показник коефіцієнта ймовірності банкрутства за допомогою моделі Е. Альтмана. У процесі розрахунку використовуються п’ять факторів (коефіцієнтів), що найбільш повно можуть охарактеризувати і фінансовий потенціал підприємства, порівняно із іншими моделями оцінки ймовірності банкрутства.

Окрім того, значною перевагою даної моделі є також можливість визначити наявність кризи на її ранніх етапах. Я вважаю, що вона має беззаперечні переваги перед іншими зарубіжними моделями.

До таких переваг можна віднести:

- простота розрахунків;

- незначна кількість показників, що забезпечують точність та якість результатів;

- доступність вихідних даних, що знаходять своє відображення у формах фінансової звітності;

- наявність логічної послідовності дослідження;

- можливість прогнозування банкрутства та визначення зони ризику, в якій знаходиться підприємство та ін.

Формула розрахунку п'ятифакторної моделі Е. Альтмана (2.1) має вигляд:

$$Z= 1,2X_1+1,4X_2+3,3X_3+0,6X_4+1,0X_5, \quad (2.1)$$

де де X_1 - відношення власного оборотного капіталу до всіх активів;

X_2 - відношення нерозподіленого прибутку до всього активів;

X_3 - відношення прибутку до виплати відсотків до всіх активів;

X_4 - відношення власного капіталу до зобов’язань;

X_5 - відношення чистого доходу до всіх активів[28].

У табл. 2.20 наведені розрахунки ймовірності банкрутства

Таблиця 2.20

Аналіз ймовірності банкрутства ТОВ «Інтеренерго Інжиніринг»

за 2020-2022 роки

Показник	Роки			2021/2020	2022/2021
	2020	2021	2022	+/-	+/-
1	2	3	4	5	6
Відношення власного оборотного капіталу до всіх активів	-0,03	0,11	0,03	0,14	-0,08
Відношення нерозподіленого прибутку до всіх активів	-0,05	0,07	0,02	0,12	-0,05
Відношення прибутку до виплати відсотків до всіх активів	2,60	6,55	1,23	3,95	-5,32
відношення власного капіталу до зобов'язань	-44,89	3,34	12,01	48,22	8,68
Відношення чистого доходу до всіх активів	0,75	2,06	1,24	1,31	-0,82
$Z= 1,2X_1+1,4X_2+3,3X_3+0,6X_4+1,0X_5$	-17,72	25,91	12,57	43,63	-13,34

За шкалою у табл. 2.21 ймовірності банкрутства визначимо стан підприємства.

Таблиця 2.21

Шкала визначення стану підприємства за моделлю Е. Альтмана

Розраховані значення критерію (індексу)	Ймовірність банкрутства
1,8	Дуже висока
1,81-2,6	Висока
2,61-2,9	Низька
2,91-3	Дуже низька

Якщо ми зіставимо дані з табл. 2.15 до 2.16, то побачимо, результати проведених розрахунків п'ятифакторною моделлю Альтмана свідчать про те, що ТОВ «Інтеренерго Інжиніринг» є фінансово стійким, а ймовірність банкрутства дуже замала. Звернемо увагу, що в 2020 році ймовірність банкрутсва була колосально висока, але вже в 2021 році показник зріс до 25,91,

проте в 2022 році він знизився до 12,57 і до критичного значення дуже далеко, сподіваємося на зростання його в наступних роках.

Далі розрахуємо показники рентабельності підприємства, які не увійшли в табл. 2.22. табл.

Таблиця 2.22

Аналіз показників рентабельності за 2020-2022 роки

Показник	Роки			2021/2020	2022/2021
	2020	2021	2022	+/-	+/-
1	2	3	4	5	6
1) рентабельності усіх активів за чистим прибутком %	0,19	19,85	0,27	19,66	-19,58
2) рентабельності необоротних активів %	83,42	4299,33	316,03	4215,91	-3983,30
3) рентабельності робочого капіталу	-5,41	184,40	10,60	189,81	-173,80
4) рентабельності реалізації	-16,79	-8,11	-1,81	8,69	6,30
5) рентабельності чистого доходу	0,25	9,62	0,22	9,37	-9,41

З табл. 2.22 можна зробити такі висновки як:

1) перший показник у 2021 році мав найвище значення серед 2020 та 2022 років. Причинами зменшення можуть бути: зниження процесу управління, збільшення суми витрат та зменшення доходів;

2) як ми можемо спостерігати показник у 2021 році значною мірою збільшився порівняно з 2020 роком. Це характеризується тим, що підприємство забезпечує достатній обсяг річного прибутку по відношенню до середньорічної вартості основних засобів компанії. Проте нажаль так не можна казати про 2022 рік так як там спостерігається велике падіння показника (рис.2.9).

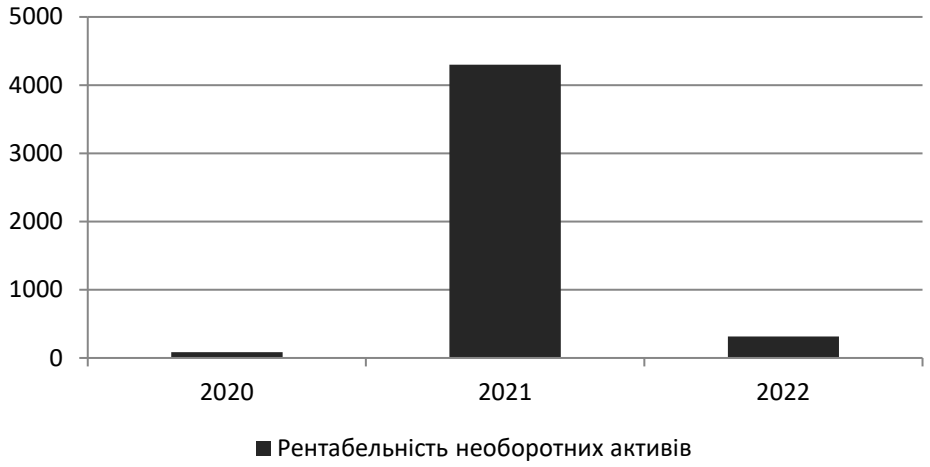

Рис.2.9. Динаміка рентабельності необоротних активів за 2020-2022 роки

3) як ми бачимо у 2020 році було взагалі від'ємне значення, але згодом у 2021 році мі вже спостерігаємо позитивне значення з відміткою 184%. Коли ми спостерігаємо показники зі знаком «-» це можна означати, що підприємство працювало собі у збиток. Але, якщо подивитися на 2022 рік, то результат дуже впав до 11% з 184% (рис.2.10).

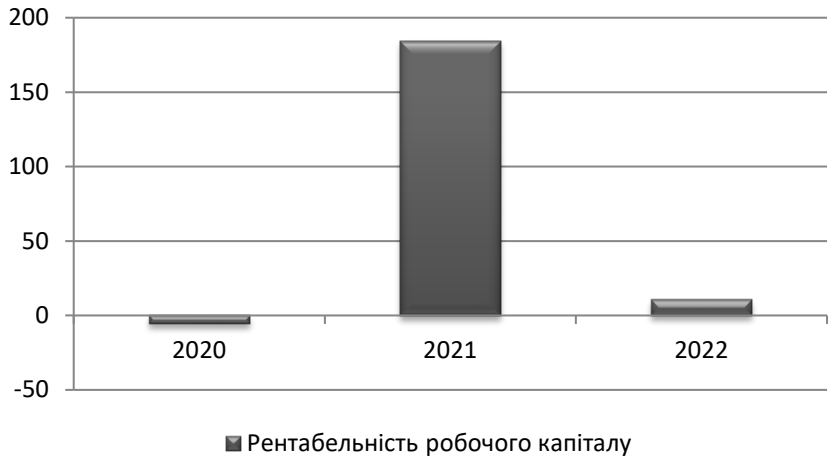

Рис.2.10. Динаміка рентабельності робочого капіталу за 2020-2022 роки

4,5) рентабельність реалізації на протязі усіх років спостерігається негативне значення, але з кожним роком воно приближається до позначки 0, та можливо вже в 2023 році зможе перетнути його і вийти на позитивний показник. Показник рентабельності чистого доходу також можна відзначити, що в 2021 році було найвище значення показника серед 2020 так 2022 роках. Різниця між 2021 та 2020 роками склала 9,37%. А що стосується 2022 року то там вона становила 9,41% .

Також для більшого наочного вигляду показників рентабельності реалізації та чистого доходу витрат пропоную роздивитись рис.2.11.

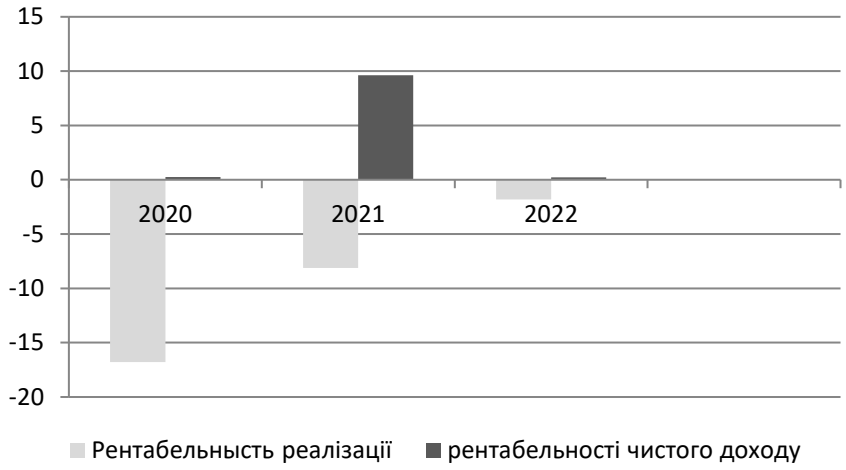

Рис. 2.11. Динаміка рентабельності реалізації та чистого доходу за 2020-2022 роки

Як можемо побачити, рентабельність впала значно у 2022, проте причини тут очевидні – через війну, підприємство не мало такого обсягу замовлень, які були до неї.

Отже, можна зробити такі висновки, які охарактеризують діяльність підприємства:

1) Науково-виробниче підприємство «Інтеренерго» було засновано у 2005 році. Відтоді воно будує «під ключ» промислові енергетичні об’єкти в різних галузях, таких як металургія, хімія, харчова промисловість. Протягом

16 років компанія використовує передові технології та найсучасніше обладнання для вирішення складних завдань будівництва та запуску промислових енергетичних об’єктів, таких як біогазові, газотурбінні та газопоршневі електростанції, тепломасляні системи та котли;

2) проведений фінансовий аналіз говорить про те, що підприємство хоч і має певні проблеми, продовжує активно розвиватись в напрямку збільшення підписання контрактів на будівництво, також з кожним роком помічається збільшення чистого доходу та чистого прибутку. Проблемними є показники рентабельності, через те, що підприємство займається будівництвом великих об’єктів, які довго реалізуються та цикл виробництва становить рік, навіть і більше. Також якщо провести черту серед 2020р., 2021р., та 2022 роком можна помітити, що більшість високих показників спостерігалась у 2021 році;

3) баланс ТОВ «Інтеренерго Інжиніринг» виявився ліквідний тому, що показники знаходяться в межах норми та намагається збільшувати свої активи з кожним роком задля покриття власних зобов’язань. Стосовно ймовірності банкрутства, то можна казати, що результати проведених розрахунків п’ятифакторною моделлю Альтмана свідчать про те, що ТОВ «Інтеренерго Інжиніринг» є фінансово стійким і вона дуже замала.

2.7. Оцінка потенційних вразливостей інформаційного середовища на підприємстві

Інформаційне середовище на підприємстві може мати різні потенційні вразливості, які можуть бути використані зловмисниками для несанкціонованого доступу до даних або завдання шкоди бізнес-процесам. Найпоширеніші вразливості інформаційної системи підприємства такі:

1. Кібератаки. Зловмисники можуть використовувати різні види кібератак, такі як DDoS-атаки (розподілений відмова у обслуговуванні), фішинг, мальвару та інші, щоб вторгнутися в системи підприємства, отримати доступ до даних або завдати шкоди.

2. Неактуалізоване програмне забезпечення. Застаріле програмне забезпечення, включаючи операційні системи та додатки, може мати вразливості, які стають доступними для зловмисників. Підприємство повинно регулярно оновлювати та патчити програмне забезпечення.

3. Слабкі паролі і недостатні методи автентифікації. Використання слабких паролів або відсутність багатофакторної аутентифікації може зробити системи більш вразливими перед атаками.

4. Несправжній соціальний інженерінг. Зловмисники можуть намагатися отримати доступ до систем, використовуючи соціальний інженерінг, шляхом обману або маніпулювання співробітниками підприємства.

5. Внутрішні загрози. Захист від внутрішніх загроз, таких як недобросовісні або недбалі співробітники, також є важливим завданням. Інсайдери можуть намагатися витягти конфіденційну інформацію або завдати шкоду системам підприємства.

6. Незашифрований обмін даними. Незашифровані дані під час передачі через мережу можуть бути підвернуті атакам або перехоплені зловмисниками.

7. Відсутність резервних копій даних. В разі втрати даних через аварію або кібератаку відсутність резервних копій може призвести до серйозних наслідків.

8. Занадто широкий доступ до даних. Надмірна кількість співробітників, які мають доступ до конфіденційних даних, може збільшити ризик витоку інформації.

9. Недостатній моніторинг та аналіз безпеки. Відсутність систем моніторингу та аналізу безпеки може призвести до несвоєчасного виявлення аномалій та інцидентів.

10. Застаріла інфраструктура. Застаріла апаратна та програмна інфраструктура може бути більш вразливою перед кіберзагрозами.

Для запобігання цим вразливостям підприємство повинно розробити та впровадити відповідну політику кібербезпеки, включаючи заходи захисту, навчання персоналу та постійний моніторинг стану безпеки.

Висновки до розділу 2

Під час написання другого розділу дипломної роботи було проаналізовано загальну характеристику діяльності підприємства ТОВ «ІНТЕРЕНЕРГО ІНЖИНІРИНГ» з метою виявлення слабких та сильних сторін зовнішнього та внутрішнього середовища підприємства. За допомогою цього вдалося зрозуміти, що фірма хоча і знаходиться на перших місцях, але конкуренти теж її наздоганяють, тому треба зосередитись на досконалості своїх можливостей у майбутньому. Наступним був проведений фінансовий аналіз ресурсів за три останні роки де були розглянуті такі показники як ділова активність, майновий стан, фінансова стійкість, прибутковість та ін., для того, щоб побачити динаміку зростання або спаду їх значень. За допомогою цього аналізу стало зрозумілим, що показники у 2022 році дуже сильно зменшилися порівняно з 2021 роком. Аналіз управління фінансовими ресурсами ТОВ «ІНТЕРЕНЕРГО ІНЖИНІРИНГ» показав, що підприємство має помірний рівень конкурентоспроможності.

Щодо стану інформаційної безпеки на підприємстві, то на сьогоднішній день забезпечення інформаційної безпеки стає стратегічним завданням для підприємства, оскільки воно повинно захищати власні активи, клієнтські дані та репутацію в умовах зростаючих загроз. Ефективна інформаційна безпека допомагає підприємствам залишатися конкурентоздатними, надійними та впевненими у своєму розвитку.

Тому незважаючи на деякі невдачі, компанія все ще робить кроки в розширенні своїх виробничих можливостей, а її чистий прибуток зростає.

РОЗДІЛ 3. РОЗРОБКА ПРОЄКТУ ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТОВ «ІНТЕРЕНЕРГО ІНЖИНІРИНГ»

3.1. Обґрунтування напрямків підвищення рівня інформаційної безпеки підприємства

Підвищення рівня інформаційної безпеки на підприємстві - це важливий процес, який вимагає комплексного підходу та залучення ресурсів і фахівців. В табл. 3.1 наведено перелік кроків і заходів, які можна розглядати для покращення інформаційної безпеки на підприємстві.

Таблиця 3.1.

Перелік можливих заходів щодо підвищення рівня інформаційної безпеки підприємства

Назва заходу	Сутність заходу
1	2
1. Аудит і аналіз поточного стану	Необхідно зрозуміти, які системи, даний інфраструктура та процеси існують на підприємстві, і як вони пов'язані з інформаційною безпекою. Проведіть аудит і визначте слабкі місця.
2. Політики та процедури	Потрібно розробити політики та процедури інформаційної безпеки для всього персоналу. Ці документи повинні визначати правила та вимоги щодо обробки і збереження конфіденційної інформації
3. Освіта та навчання	Необхідно забезпечте навчання та підвищення кваліфікації персоналу щодо правил інформаційної безпеки, включаючи усвідомлення загроз та як їх уникати
4. Захист мережі	Потрібно встановити засоби захисту мережі, такі як брандмауери, антивіруси, системи виявлення та запобігання вторгненням (IDS/IPS), а також системи керування доступом.
5. Шифрування	Необхідно використовувати шифрування для захисту конфіденційних даних під час передачі і зберігання
6. Резервне копіювання і відновлення даних	Регулярно потрібно створювати резервні копії даних і розробляйте плани відновлення в разі втрати даних або катастрофи
7. Моніторинг і аналіз подій	Потрібно встановити системи моніторингу і аналізу подій для виявлення надзвичайних подій або вторгнень

Закінчення табл. 3.1

1	2
8. Фізична безпека	Необхідно захищайти фізичний доступ до інформаційних ресурсів шляхом обмеження доступу до серверних кімнат і інших важливих місць
9. Аутентифікація та авторизація	Потрібно використовувати сильну аутентифікацію та встановлюйте правила авторизації для керування доступом до систем і даних
10.Управління ризиками	Необхідно проводити оцінку ризиків та розробляти стратегію управління ризиками для визначення пріоритетів і заходів для зменшення загроз
11.Звітність і відповідність	Потрібно дотримуватияь законодавства та регуляторних вимог і забезпечувати ведення звітності про інформаційну безпеку
12.Тестування і аудит	Необхідно регулярно проводити тестування на проникнення, аудити та перевірки інформаційної безпеки
13.Спостереження за трендами у загрозах	Потрібно слідкувати за новими загрозами і розробляти плани дій для їх протидії
14.Постійне вдосконалення	Так як інформаційна безпека це процес, який постійно розвивається. Потрібно постійно оцінювати та вдосконалювати існуючу стратегію інформаційної безпеки.
15.Захист на рівні постачальників	Необхідно вимагати від постчальників та партнерів дотримуватися стандартів інформаційної безпеки

Отже, в табл. 3.1. наведено загальний перелік заходів, спрямованих на підвищення інформаційної безпеки підприємства. Конкретні кроки залежать від проведеного аудиту на підприємстві, обсягу даних і інших факторів. Розробка і реалізація стратегії інформаційної безпеки повинна бути індивідуальною та орієнтованою на потреби конкретного бізнесу.

3.2. Програма заходів щодо підвищення рівня інформаційної безпеки на підприємстві

Заходи щодо зниження ризиків і забезпечення безпеки в цифровому середовищі включають наступні заходи:

1. Використання антивірусного та антиспам-програмного забезпечення. Встановлення та оновлення антивірусних та антиспам-засобів допомагає виявляти та запобігати вторгненням зловмисників та відправці спаму.

2. Захист доступу та автентифікація. Вимагання сильних паролів та використання двофакторної аутентифікації зменшують ризик несанкціонованого доступу.

3. Шифрування даних. Використання шифрування даних у спокійному та транзитному стані забезпечує конфіденційність інформації під час передачі та зберігання.

4. Регулярні оновлення та патчі. Постійне оновлення операційних систем, програмного забезпечення та апаратних засобів є важливим для закриття вразливостей та запобігання кібератак.

5. Сегментація мережі. Розділення мережі на окремі сегменти та використання брандмауера допомагає обмежити поширення можливих загроз усередині компанії.

6. Захист від соціальної інженерії. Навчання персоналу та здійснення обізнаних рішень у відповіді на фішингові атаки та інші форми соціальної інженерії.

7. Регулярні аудити та моніторинг безпеки. Проведення аудитів та постійний моніторинг систем безпеки для вчасного виявлення аномалій та інцидентів.

8. Запасні копії даних та відновлення систем: Регулярне створення та зберігання резервних копій даних допомагає відновити інформацію в разі катастрофи або кібератаки.

9. Політика та освіта з кібербезпеки. Розроблення політики кібербезпеки та навчання персоналу її дотримуватися.

10. Запобігання витоку інформації. Встановлення заходів для запобігання витоку конфіденційної інформації, включаючи обмеження прав доступу. Ці заходи допомагають компаніям знизити ризики та забезпечити безпеку в цифровому середовищі, забезпечуючи надійність та конфіденційність інформації.

3.3. Запровадження проєкту контролю за клієтськими комп'ютерами в локальних та зовнішних мережах

Мета розробки та використання системи: моніторинг клієнтів, які знаходяться поза межами організації (локальної мережі, або ВПН) на предмет оновлень операційної системи та антивірусу, встановленного ПЗ, активованого ПЗ Бітлокер.

Клієнти, які є не підключеними до вашої внутрішньої мережі. Переваги використання:

повний контроль серверів і ролей, що надають послугу

немає залежності від хмарних служб

може не вимагати віртуальної приватної мережі (VPN)

усі витрати пов'язані з локальною послугою

Через вищі вимоги до безпеки для керування клієнтськими комп'ютерами в публічній мережі це вимагає використання сертифікатів PKI. Ця конфігурація забезпечує автентифікацію підключень незалежним органом. Коли клієнти і сервери сайту надсилають дані, вони зашифровані та безпечні.

Опис системи (рис. 3.1):

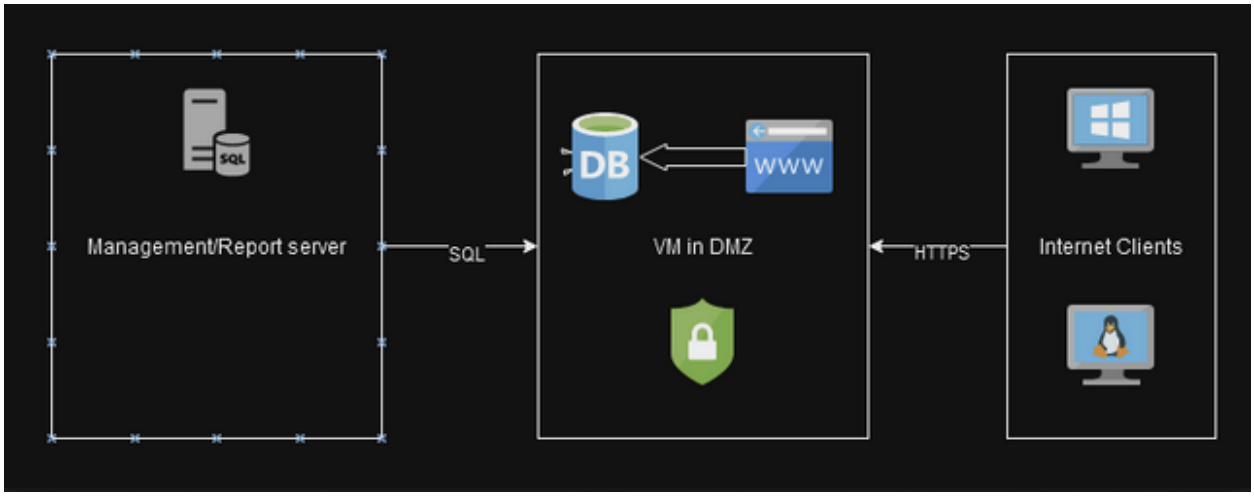

Рис. 3.1. Схема організації надходження інформації до бази даних (БД)

База даних контролю та сайт керування знаходиться в мережі периметра. Ця мережа також має контролер домену для читання для автентифікації користувача. Брандмауер між периметром і внутрішніми мережами забезпечує безпеку.

Клієнт надсилає забрані дані на сайт за допомогою протоколу HTTPS. Сайт приймає і записує дані в БД після перевірки валідності.

Сервер основної БД та керування забирає дані з тимчасової БД в небезпечній зоні в свою безпечну БД, до якої звертається персонал керування в захищеній мережі.

Конфігурація використовується в таких сценаріях:

Для комп'ютерів, які, як ви знаєте, ніколи не під'єднаються до вашої внутрішньої мережі. Наприклад, комп'ютери в точках продажу у віддалених місцях. Щоб обмежити зв'язок клієнта лише за протоколом HTTPS. Наприклад, для підтримки брандмауера та політики обмеженої безпеки.

Для повного керування клієнтськими ПК всередині захищенної мережі буде використовуватися безкоштовний комплекс Tactical RMM.

Tactical RMM – це безкоштовна RMM з відкритим кодом, створена за допомогою Django, Vue і Golang. Він має агент Windows і інтегрується з MeshCentral (рис. 3.2).

Він містить багато функцій, які ви очікуєте від RMM, наприклад:

віддалене керування робочим столом, яке вони здійснюють через MeshCentral;

керування виправленнями Windows;

віддалене виконання команд і сценаріїв (скрипти Powershell, пакетні та Python);

автоматичні перевірки, які можуть сповіщати вас електронною поштою або SMS (ЦП, диск, пам'ять, журнал подій тощо);

інвентаризація обладнання та програмного забезпечення

виконання завдань/скриптів за розкладом

Встановити програмне забезпечення віддалено через Chocolatey

Управління послугами

Віддалена оболонка в реальному часі і т.д.

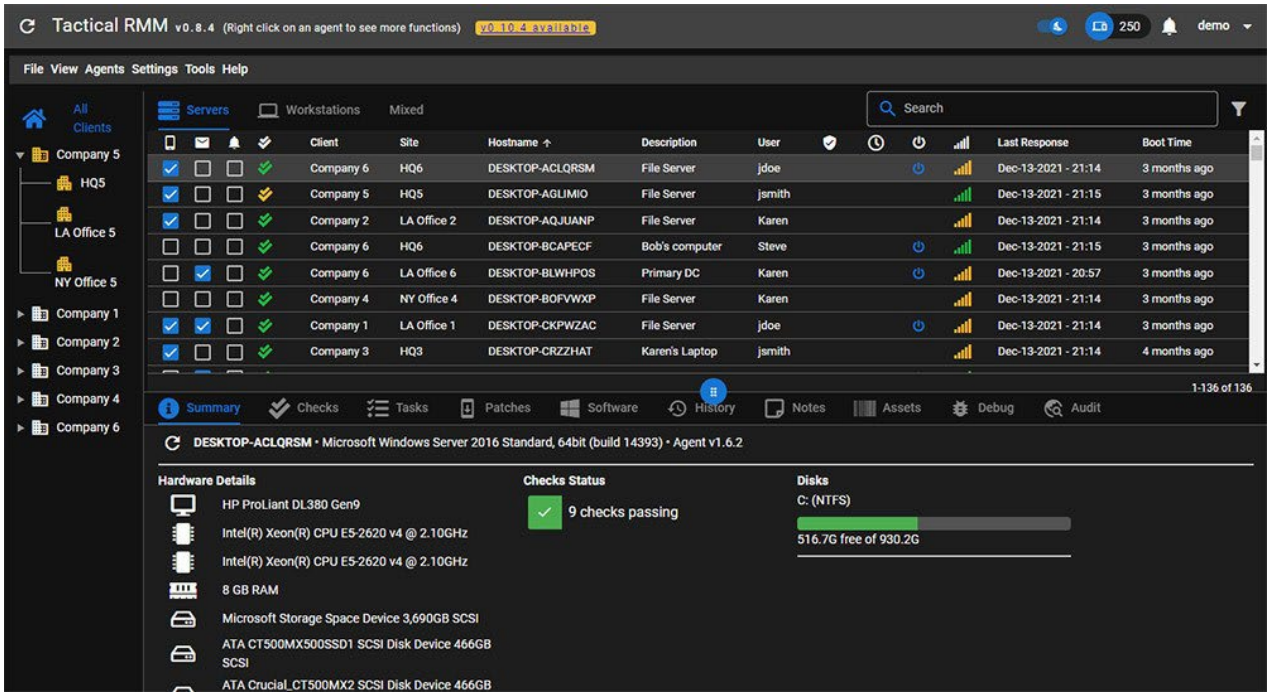

Рис. 3.2. Скріншот ПЗ Tactical RMM

Основні переваги використання ПЗ Tactical RMM на ТОВ «Інтеренерго Інжиніринг»:

1) оскільки функціональність великих продуктів RMM продовжує зростати, вони також ускладнюються. З огляду на те, що назавжди вибрано стільки функцій, іноді здається, що варто почати з нуля, пам’ятаючи про поточні функції.

2) другою великою перевагою Tactical RMM є те, що він свіжий, чистий і потужний. Хоча він не може зрівнятися з набором функцій великих продуктів, які створювали протягом десяти років, він добре справляється з основними завданнями.

Оскільки він є продуктом з відкритим кодом, він дає вам більше можливостей контролю. Компанія буде менше залежити від підвищення цін, видалення функцій або змін умов. Або ваш RMM купується, продається, скасовується або поглинається.

Коли MSP думають про персоналізацію, вони часто звертають увагу на поверхневі аспекти, як-от логотипи та інформаційні панелі, але справжня персоналізація полягає в налаштуванні RMM відповідно до вашого робочого процесу. Оскільки ми маємо відкритий код, ми маємо можливість форкувати кодову базу Tactical RMM і адаптувати її для наших потреб.

Отже, запровадження запропонованої системи дозволить значно підвищити інформаційну безпеку компанії і відповідність до вимог клієнтів у майбутньому.

3.4. Оцінка економічної ефективності запропонованих заходів з урахуванням ризиків

Під час запровадження проєкту встановлення контролю за клієтськими комп'ютерами в локальних та зовнішних мережах необхідно купити новий сервер, вартість якого складає 100 тис. грн. Для оцінки економічної ефективності проекти використовують такі показники, як чистий дисконтований дохід, індекс доходності та період окупності інвестицій. Дані критерії базуються на дисконтуванні грошових потоків і є визнаними у світовій практиці основними показниками, що акумулюють вигоди від впровадження інвестиційного проекту. Саме їхній розрахунок, в першу чергу, вказує на економічну ефективність інвестиційного проекту.

1. Чистий дисконтований дохід. Дає змогу отримати абсолютну величину ефекту від реалізації проекту.

$$ЧДД = -К + \frac{ΔП1}{(1+i)^1} + \frac{ΔП2}{(1+i)^2} + \frac{ΔП3}{(1+i)^3}, \quad (3.1)$$

де К- капітальні витрати, грн.;

і – ставка дисконту.

ΔП – чистий прибуток, грн.;

Ставка дисконту розраховується за формулою Фішера:

$$\text{і} = \text{а} + \text{в} + \text{в} * \text{а}, \tag{3.2}$$

де а – рівень інфляції;

в – ставка по депозиту.

Згідно до Закону України «Про Державний бюджет України на 2024 рік» індекс інфляції в Україні в 2024 році планується на рівні 9,7%. Середня ставка за депозитами – 10,5% (Приватбанк).

$\text{І} = 0{,}097 + 0{,}105 + 0{,}105 * 0{,}097 = 0{,}212.$

2. Період окупності проекту розрахуємо за формулою:

$$\text{ПО} = \frac{\text{К}}{\text{СГДП}}, \tag{3.3}$$

де К – капітальні витрати, грн.;

СГДП – середньорічний грошовий потік, грн.

СГДП – розраховується за формулою:

$$\text{СГДП} = \frac{\text{ГП}}{n}, \tag{3.4}$$

n – період реалізації проекту.

3. Індекс доходності проекту розраховується за формулою:

$$\text{ІД} = \frac{\text{ГП}}{\text{К}}, \tag{3.5}$$

Загальна сума інвестицій, пов’язана з реалізацією проєкту наведено в табл. 3.2.

Таблиця 3.2.

Розрахунок інвестицій для запровадження проєкту посилення рівня інформаційної безпеки на ТОВ «Інтеренерго Інжтніринг»

Назва обладнання	Необхідна кіль-ть	Вартість одиниці, тис. грн	Разом, тис. грн
1. Сервер	2	110	220
2. Блок безперебійного живлення для кожного сервера, який буде забезпечувати автоматичну роботу протягом 4-х годин	2	215	430
РАЗОМ			650

Розрахуємо економічну ефективність від технологічного заходу – Щорічна сума приросту замовлень (заключення контрактів) через збільшення довіри клієнтів через відповідність вхідним параметрам інформаційної безпеки становить 317091,25 грн.

$$\text{ЧДД} = -650000 + \frac{317091{,}25}{(1+0{,}212)^1} + \frac{317091{,}25}{(1+0{,}212)^2} + \frac{317091{,}25}{(1+0{,}212)^3} + \frac{317091{,}25}{(1+0{,}212)^4} + \frac{317091{,}25}{(1+0{,}212)^5} = 213901{,}08 \text{ грн.}$$

$$\text{СГДП} = \frac{863901{,}08}{5} = 172780{,}22 \text{ грн.}$$

$$\text{ПО} = \frac{650000}{172780{,}22} = 3{,}76 \text{ років.}$$

$$\text{ІД} = 863901{,}08 = 1{,}32 \text{ грн/грн.}$$

Таким чином, можна зробити висновок про ефективність даного проекту, адже чистий дисконтований дохід дорівнює 213901,08 грн, індекс

доходності дорівнює 1,32 грн/грн, а період окупності проекту 3 роки 9 місяців роки.

Реалізація проекту пов’язана з ризиком, адже на реалізацію будь-якого проекту впливає ряд зовнішніх та внутрішніх факторів. Тому для зменшення невизначеності потрібно виявити та оцінити ризики, що можуть виникнути при реалізації проекту. Найнебезпечнішими ризиками для проекту є ті ризики, на які підприємство не може вплинути, а саме зовнішні ризики, такі як, наприклад, зміна показника індексу інфляції. Тому їх необхідно враховувати при обґрунтуванні доцільності впровадження інвестиційного проекту.

Для визначення ризиків реалізації проекту застосуємо метод експертних оцінок. Даний метод заснований на опитуваннях кваліфікаційних спеціалістів і подальшій обробці результатів опитування. Був складений перелік факторів ризику, на основі чого була складена анкета з 12 питань. Приклад анкети опитування наведено у дод. Б (табл. Б.1). Необхідно дати оцінку (від 1 до 10) кожному виду ризиків та вказати вірогідність кожного ризику.

Для визначення ризикованості проекту скористаємось методикою оцінки ризиків за методологією Денисенка Н.П.

Результати опитування наведені у дод. А (табл. Б.2).

На основі отриманих результатів була розрахована середня вірогідність настання окремого виду ризику як середньоарифметична величина вірогідностей, а також сумарна оцінка кожного виду ризику з урахуванням середньої вагомості ризику (табл. 3.3).

Таблиця 3.3

Оцінка ризикованості запропонованого заходу

№	Види ризику	Середня вагомість ризику	Сумарна оцінка
1	2	3	4
Проектні ризики передінвестиційної фази:			19,7
1	Помилка в прогнозуванні ринків збуту продукції	0,57	11,90
2	Помилка у плануванні та проектуванні заходів	0,43	7,80

Закінчення табл. 3.3

1	2	3	4
Проектні ризики інвестиційної фази:			18,32
3	Зміна вартості обладнання внаслідок коливань курсу іноземної валюти	0,43	9,10
4	Невиконання термінів поставки обладнання	0,17	2,67
5	Несправність поставленого обладнання	0,25	4,00
6	Відмова постачальників від попередньо укладених контрактів	0,15	2,55
Проектні ризики експлуатаційної фази:			18,32
7	Підвищення вартості матеріальних ресурсів	0,23	3,97
8	Виробничо-технологічний ризик пов'язаний з недостатністю або якістю робочої сили	0,13	2,13
9	Поява нових конкурентів	0,15	3,00
10	Виробничо-технологічний ризик пов'язаний з виробничим браком	0,20	4,00
11	Вихід з ладу старого обладнання	0,08	1,42
12	Зміна податкової політики країни	0,20	3,80
Усього по трьом фазам			56,33

В якості експертів виступають провідні спеціалісти підприємства, керівні посади, ТОП- менеджери та менеджери середнього рівня, серед яких керівники та заступники планово-економічного відділу, виробничого цеху, головний інженер та інші.

Оскільки у анкеті 12 факторів ризику, то відповідно максимальна величина ризику складе 120, а мінімальна – 12.

Тоді ступінь ризику реалізації бізнес-плану може знаходитися у наступних інтервалах:

12 - 48 – мало ризикований проект;

49 - 84 – середньо ризикований проект;

85 - 120 – значно ризикований проект.

З табл. 3.4 загальна зважена оцінка складає 56,33. Отже, запропонований захід відноситься до категорії середньо ризикованих.

Для більш наглядного впливу кожного ризику на проведення заходів підвищення ефективності діяльності підприємства спроектована роза ризиків (рис. 3.3).

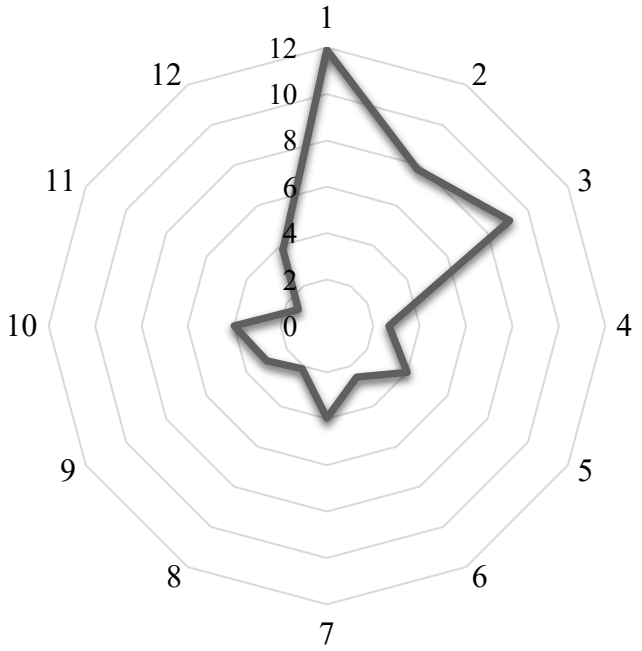

Рис. 3.3. Роза ризиків заходу

З рис. 3.3 бачимо, що найбільшої уваги слід приділити прогнозуванню ринків збуту продукції та чіткому плануванню та проектуванню заходів. Необхідно правильно оцінити кількість потенційних контрактів підприємства та врахувати можливі обмеження.

Висновки до розділу 3

Для посилення рівня економічної безпеки було запроваджено проєкт контролю за клієтськими комп'ютерами в локальних та зовнішніх мережах. Основною метою розробки та використання системи є: моніторинг клієнтів, які знаходяться поза межами організації (локальної мережі, або ВПН) на предмет оновлень операційної системи та антивірусу, встановленого ПЗ, активованого ПЗ Бітлокер. Завдяки цьому проєкту забезпечується безпека з роботою з клієнти, які є не підключеними до внутрішньої мережі. Переваги використання: повний контроль серверів і ролей, що надають послугу; немає залежності від хмарних служб; може не вимагати віртуальної приватної мережі (VPN); усі витрати пов'язані з локальною послугою.

Також було оцінено економічну ефективність запропонованого заходу, можна зробити висновок про ефективність даного проекту, адже чистий дисконтований дохід дорівнює 213901,08 грн, індекс доходності дорівнює 1,32 грн/грн, а період окупності проекту 3 роки 9 місяців роки.

Під час запровадження проєкту забезпечення підвищення рівня інформаційної безпеки було використано метод експертного оцінювання. В якості експертів виступали провідні спеціалісти підприємства, керівні посадовці, ТОП- менеджери та менеджери середнього рівня, серед яких керівники та заступники планово-економічного відділу, виробничого цеху, головний інженер та інші. За результатами оцінки загальна зважена оцінка складає 56,33. Отже, запропонований захід відноситься до категорії середньо ризикованих.

Щодо ризиків запропонованого проєкту, то найбільшої уваги слід приділити прогнозуванню ринків збуту продукції та чіткому плануванню та проектуванню заходів. Необхідно правильно оцінити кількість потенційних контрактів підприємства та врахувати можливі обмеження.

ВИСНОВКИ

У сучасних умовах динамічного бізнес-середовища одним із ключових аспектів забезпечення стійкого зростання бізнесу та формування позитивних результатів фінансової діяльності є створення ефективної системи інформаційної безпеки на підприємстві. В першому розділі дипломної роботи було доведено, що підвищення рівня інформаційної безпеки на підприємстві – це важливий процес, який вимагає комплексного підходу та залучення ресурсів і фахівців.

Підвищення рівня інформаційної безпеки на підприємстві є критично важливою необхідністю в сучасному бізнес-середовищі. Це визначається рядом факторів, які включають зростання загроз кібербезпеки, збільшення обсягу цифрової інформації та важливість ефективного використання цієї інформації для бізнес-процесів. Ось кілька ключових аспектів, які роблять підвищення рівня інформаційної безпеки обов'язковим: захист від кіберзагроз; конфіденційність інформації; забезпечення цілісності даних; забезпечення доступності інформації; дотримання законодавства та регуляцій; збереження репутації. Підвищення рівня інформаційної безпеки є ключовим елементом для збереження довіри клієнтів і партнерів.

За результатами проведеного аналізу у другому розділі, можна відмітити наступне те, що фірма хоча і знаходиться на перших місцях, але конкуренти теж її наздоганяють, тому треба зосередитись на досконалості своїх можливостей у майбутньому. Наступним був проведений фінансовий аналіз ресурсів за три останні роки де були розглянуті такі показники як ділова активність, майновий стан, фінансова стійкість, прибутковість та ін., для того, щоб побачити динаміку зростання або спаду їх значень. За допомогою цього аналізу стало зрозумілим, що показники у 2022 році дуже сильно зменшилися порівняно з 2021 роком. Аналіз управління фінансовими ресурсами ТОВ «ІНТЕРЕНЕРГО ІНЖИНІРИНГ» показав, що підприємство має помірний рівень конкурентоспроможності.

Щодо стану інформаційної безпеки на підприємстві, то на сьогоднішній день забезпечення інформаційної безпеки стає стратегічним завданням для підприємства, оскільки воно повинно захищати власні активи, клієнтські дані та репутацію в умовах зростаючих загроз. Ефективна інформаційна безпека допомагає підприємствам залишатися конкурентоздатними, надійними та впевненими у своєму розвитку. Тому незважаючи на деякі невдачі, компанія все ще робить кроки в розширенні своїх виробничих можливостей, а її чистий прибуток зростає.

Для підвищення економічної безпеки у третьому розділі був запропонований до впровадження проєкт контролю за комп'ютерами клієнтів у локальних та зовнішніх мережах. Головною метою цієї системи є моніторинг клієнтів, що перебувають поза організаційною мережею (локальною мережею або ВПН). Завдяки цьому проєкту забезпечується безпека в роботі з клієнтами, які не знаходяться в межах внутрішньої мережі. Переваги використання включають повний контроль над серверами та ролями, які надають послугу; незалежність від хмарних служб; можливість обійтися без віртуальної приватної мережі (VPN); усі витрати пов'язані з локальним обслуговуванням.

Ефективність запропонованого заходу була оцінена з економічного погляду, і проект виявився ефективним, оскільки чистий дисконтований дохід становить 213901,08 грн, індекс доходності дорівнює 1,32 грн/грн, а період окупності складає 3 роки 9 місяців. Під час впровадження проєкту з підвищення рівня інформаційної безпеки використовувався метод експертного оцінювання з участю провідних спеціалістів та керівництва підприємства. Оцінка ефективності показала, що загальна зважена оцінка становить 56,33, класифікуючи запропонований захід як середньо ризикований. Щодо ризиків проєкту, особлива увага має бути приділена прогнозуванню ринків збуту та точному плануванню заходів. Оцінка кількості потенційних контрактів та урахування можливих обмежень також є ключовими аспектами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонова С. Є. Інформаційна безпека / С. Є. Антонова, Г. Ф. Мартинюк // Державне управління: удосконалення та розвиток. – 2019. – № 11. – Режим доступу: http://www.dy.nayka.com.ua/pdf/11_2019/38.pdf.

2. Асєєва Л. А. Оцінка ризиків конфіденційності інформаційної безпеки проектів на основі нечіткої логіки / Л. А. Асєєва, О. М. Шушура // Телекомунікаційні та інформаційні технології. – 2021. – № 1. – С. 88-95.

3. Барановський О. І. Фінансова безпека. Київ : Фенікс, 2009. – 338 с.

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

5. Боднар І. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки, 2014, № 1. С 68-75.

6. Боднар І. Р. Пріоритетні напрями держави в сфері інформаційної безпеки / І. Р. Боднар // Економіка & держава. – 2012. – № 2. – С. 27-29.

7. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.

8. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (29), 2015 р. С.56-61. URL : https://core.ac.uk/download/pdf/47240087.pdf

9. Войнаренко М. П. Інформаційні системи і технології в управлінні організацією : навч. посіб. / М. П. Войнаренко, О. М. Кузьміна, Т. В. Янчук. – Вінниця : Центр підготовки наукових та навчально-методичних видань ВТЕІ КНТЕУ, 2015. – 496 с.

10. Волот О. І. Інформаційна та кібернетична безпека сучасного підприємства: забезпечення та моделювання / О. І. Волот // Центральнонауковий вісник. Економічні науки. – 2019. – № 3(36). – С. 238-247.

11. Виговська О., Бєлоусова Н. Інформаційна складова національної безпеки України : кол. монографія / Ін-т міжнар. відносин, Київ. нац. ун-т ім. Тараса Шевченка, Київ. ун-т ім. Бориса Грінченка. Київ : Київ. ун-т ім. Б. Грінченка, 2017. 166 с.

12. Гнатцов О. Г. Інформаційні ресурси в системі забезпечення державної безпеки / О. Г. Гнатцов. – Режим доступу: http:// www.niisp.gov.ua/vydanna/panorama

13. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. Посібник. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.

14. Дейнега О. В. Інформаційна безпека підприємств в умовах глобалізації 4.0 / О. В. Дейнега // Економіка та суспільство. – 2019. – № 20. – С. 19.

15. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об’єктам інформаційної безпеки / В. Н. Дереко //Інформаційнабезпекалюдини,суспільства,держави.–2015.–№2.–С.16-22.

16. Державний стандарт України Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96 [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id=38836

17. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://www.zakon3.rada.gov.ua/laws/ show/514/2009

18. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту / В. В. Домарев. – Режим доступу:http://domarev.kiev.ua

19. Економічна безпека підприємств, організацій та установ: навчальний посібник / Ортинський В. Л., Керницький І. С., Живко З. Б. та ін. К. : Правова єдність, 2009. – 544 с.

20. Жарков Я. М., Бєсєдіна Л. М. Напрямки зовнішнього інформаційно-психологічного впливу на Україну. Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. 2009. – № 19. – С. 15-19.

21. Захаренко К. Розвиток системи інформаційної безпеки: досвід зарубіжних країн / К. Захаренко // Вища освіта України. – 2018. – № 3. – С. 71-77.

22. Зубок М.І. Інформаційна безпека в підприємницькій діяльності / М.І. Зубок. – Київ : ГНОЗІС, 2015 – 216 с.

23. Інформаційна безпека. Підручник В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.

24. Інформаційна безпека суспільства і держави. Стратегічні цілі і задачі інформаційної боротьби. – Режим доступу: http://www.ngo.dn.ua/doc/concept.doc

25. Концепція інформаційної безпеки України. [Електронний ресурс] –Режим доступу: http://mip.gov.ua/files/banners/Final%20%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D1%96%D1%97%20(%D0%A2%D0%B5%D0%BA%D1%81%D1%82)%20-%2030.09.15.pdf

26. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. … докт. юрид. наук : спец. 12.00.07. М-во освіти і науки України, Нац. ун-т внутр. справ. Харків. ХНУВС, 2004. – 42 с.

27. Корпоративні інформаційні системи : навч. посіб. / С. А. Яремко, К. В. Копняк, О. М. Кузьміна, Л. П. Половенко. – Вінниця : Редакційно-видавничий відділ ВТЕІ КНТЕУ, 2020. – 256 с.

28. Лахман О. Проблеми захисту інформації на підприємстві / О. Лахман // Вісник студентського наукового товариства "Ватра" Вінницького

торговельно-економічного інституту Київського національного торговельно-економічного університету : за матеріалами III Всеукраїнської студент. наук.-практ. конференції "Актуальні проблеми ефективного соціально-економічного розвитку України: пошук молодих", 24 квітня 2014 року. – Вінниця : Центр підготовки наукових та навчально-методичних видань ВТЕІ КНТЕУ, 2014. – Вип.17. – С. 519-522.

29. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К. : КНТ, 2006. 280 с. URL: http://pidruchniki.com/component/option,com_jdownloads/Itemid,999999/catpid,349/task,view.annotation

30. Литвиненко А. О. Інформаційна безпека як складовий елемент системи економічної безпеки суб'єкта підприємництва / А. О. Литвиненко, Є. М. Іполітов // Стратегічні пріоритети розвитку підприємництва, торгівлі та біржової діяльності : матеріали IV-ої Міжнародної науково-практичної конференції, 10-11 травня 2023 р. – Запоріжжя, 2023. - С. 74-75

31. Литвинов В.В. Моделювання та аналіз безпеки розподілених інформаційних систем: навч. пос. [для студ. спец. 121 «Інженерія програмного забезпечення»] / В.В. Литвинов, В.В. Казимир, І.В. Стеценко та ін. – Чернігів: Чернігів. нац. технол. ун-т, 2016. – 254 с.

32. Маркіна І. А. Інформаціи на безпека підприємства та організаціині заходи ї ї забезпечення / І. А. Маркіна, Ю. М. Гарічев // Українськии журнал прикладної економіки. – 2019. – Том 4. – № 4. – С. 209–215.

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

34. Морозов О. Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності / О. Л. Морозов. – Режимдоступу:http://www.viche.info

35. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

36. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

37. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука – Харків: 2018. – 289 с. [Електронний ресурс]. – Режим доступу: https://cutt.ly/5ugjj6s

38. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. Юридичний журнал. – 2009. – № 5. – С. 122-134.

39. Питання концепції реформування інформаційного законодавства України / Калюжний Р., Говловський В., Цимбалюк В., Гузалюк М. К. : НТУУ «КПІ», Міністерство освіти і науки України, 2000. – С. 17-21.

40. Прав Р. Ю. Протидія зовнішнім інформаційним загрозам в Україні / Р. Ю. Прав // Інвестиції: практика та досвід. – 2020. – № 2. – С. 141-145.

41. Про Концепцію Національної програми інформатизації. Закону України від 4 лютого 1998 р. № 75/98-ВР // Відомості ВерховноїРади.–1998.–№27-28.–С.182.

42. Про національну безпеку України Закон України від 21.06.2018 № 2469-VIII // Відомості Верховної Ради. – 2018. – № 31. – Ст. 241.

43. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. URL : https://zakon.rada.gov.ua/laws/show/537-16#Text

44. Рижук О. М. Інформаційна безпека України в умовах глобалізаційних викликів та гібридної війни : монографія / за ред. Бебика В.М. ; Відкр. міжнар. ун-т розвитку людини «Україна». Київ : Університет «Україна», 2019. 177 с.

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

46. Соснін О. В. Інформаційна політика України: проблеми розбудови / О. В. Соснін. – Режим доступу: http://www.niisp.gov.ua/vvdanna/panorama

47. Степко О.М. Аналіз головних складових інформаційної безпеки держави / О.М. Степко // Науковий вісник Інституту міжнародних відносин НАУ. – Сер. : Економіка, право, політологія, туризм. – К. : Вид-во Нац. авіац. ун-ту "НАУ-друк", 2011. – Вип. 1(3). – С. 90-99.

48. Стецюк В. Інформаційна безпека підприємства / В. Стецюк // Світоглядні трансформації особистості студента ВНЗ: історико-філософські, соціально-правові та мовознавчі аспекти : збірник тез доповідей III студентської науково-практичної інтернет-конференції 25 травня 2016 р. – Вінниця : ВТЕІ КНТЕУ, 2016. – С. 90-94.

49. Турчак А. Основні складові інформаційної безпеки держави / А. Турчак. // Аспекти публічного управління. – 2019. – Том 7 № 5. – С. 44-56.

50. Чернишова Л. О. Світовий ринок інформаційно-комунікаційних технологій: тенденції та перспективи розвитку / Л. О. Чернишова, Л. В. Новікова // Підприємництво та інновації. – 2021. – № 16. – С. 15-19. – Режим доступу: http://www.ei-journal.in.ua/index.php/journal/article/view/396/384.

51. Чуруброва С. М. Політика інформаційної безпеки в системах інформаційно-аналітичного забезпечення підтримки прийняття організаційних рішень / С. М. Чуруброва // Проблеми програмування. – 2016. – № 4. – С. 97-103.

52. Rybalchenko L., Kosychenko O., Klinytskyi I. Ensuring economic security of enterprises taking into account the peculiarities of information security. Scientific journal «Philosophy, Economics and Law Review». 2022. Vol. 2 (1). Pp. 71-81.

53. The Security Risk Management Guide. Microsoft Corporation, 2006. [Електронний ресурс]. – Режим доступу : http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default (дата обращения —20.11.2023).

ДОДАТКИ

Додаток А

Публікація тез доповіді на конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Кафедра підприємництва, торгівлі та біржової діяльності

СТРАТЕГІЧНІ ПРІОРИТЕТИ РОЗВИТКУ ПІДПРИЄМНИЦТВА, ТОРГІВЛІ ТА БІРЖОВОЇ ДІЯЛЬНОСТІ

Матеріали IV-ої Міжнародної науково-практичної конференції
(10-11 травня 2023 року)

м. Запоріжжя
2023

Продовження дод. А

Литвиненко А. О.[1], Іпполітов Є. М. [2]
[1]к.е.н., доц. кафедри підприємництва і торгівлі, Харківський національний економічний університет імені Семена Кузнеця, м. Харків, Україна
[2] здобувач вищої освіти, Харківський національний економічний університет імені Семена Кузнеця, м. Харків, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВИЙ ЕЛЕМЕНТ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ СУБ'ЄКТА ПІДПРИЄМНИЦТВА

Економічна безпека – це стан і здатність економічної системи протистояти небезпеці руйнування її оргструктури і статусу, а також перешкодам у досягненні мети розвитку. Її можна окреслити як стан підприємства в межах граничних значень і здатність протидіяти загрозам та забезпечувати реалізацію економічних інтересів [1]. Організацією забезпечення безпеки переставлених об'єктів економічної безпеки займаються окремі особи, підрозділи, служби, органи, відомства та установи – суб'єкти безпеки. На думку Іванюти Т.М., всіх суб'єктів економічної безпеки підприємства можна виокремити в дві групи [2]:

Перша група суб'єктів складається зі структури самого підприємства, на яку покладено забезпечення його безпеки. Друга група – суб'єкти, які знаходяться за межами підприємства та не підпорядковуються його керівництву. Це передусім державні органи, що створюють умови забезпечення безпеки підприємства.

Для управління економічною безпекою підприємства важливим аспектом є визначення основних її складових. Складові економічної безпеки підприємства – це сукупність основних напрямів його економічної безпеки, істотно відмінних один від одного за своїм змістом. Під час дослідження складових економічної безпеки, що виокремлюються різними науковцями, авторами було їх узагальнено та надано сутнісну характеристику [3,4]: фінансова – демонструє стан найбільш ефективного використання фінансових ресурсів; техніко-технологічна – характеризує рівень технології, що використовується суб'єктом підприємництва; кадрово-інтелектуальна – полягає у збереженні та розвитку кадрового й інтелектуального потенціалу підприємства, політико-правова – стосується дотримання підприємством і його співробітниками всіх аспектів діючого законодавства; екологічна – дотримання екологічних норм технології і випуску продукції; інтерфейсна – характеризує надійність взаємодії з економічними контрагентами; інформаційна – захист комерційної таємниці й конфіденційної інформації; комп'ютерна безпека. З розвитком цифровізації бізнесу, запровадження суб'єктами підприємництва електронної комерції, зростає необхідність в захисті як персональних даних клієнтів так і фінансових документів, клієнтської бази та інших важливих складових безпечної діяльності. Тому,

необхідно здійснювати захист інформації на таких засадах: захист інформації має організувати і проводити власник інформації або уповноважені ним особи; захистом інформації власник зможе охороняти свої права на володіння і розпорядження інформацією, прагне захистити її від незаконного заволодіння і використання на шкоду його інтересам; захист інформації здійснюється шляхом обмеження доступу та створення умов, що виключають або суттєво ускладнюють несанкціонований, незаконний доступ до інформації та її носіїв.

Захист інформації представляє собою діяльність власника інформації або уповноваженої ним особи з: забезпечення своїх прав на володіння, розпорядження і управління захищеною інформацією; запобігання витоку і втрати інформації; збереження повноти, вірогідності, цілісності захищеної інформації, її масивів і програм обробки; збереження конфіденційності або таємності захищеної інформації, відповідно до правил, установлених законодавчими й іншими нормативними актами.

Отже, в умовах нестабільності зовнішнього середовища формування надійної системи економічної безпеки підприємства можливе лише за системного підходу до її організації. Завдяки цій системі має бути забезпечено можливість оцінювання перспектив розвитку та зростання суб'єкта підприємництва, розроблення тактики і стратегії його розвитку, зменшення наслідків впливу зовнішнього середовища, а також попередження можливостей виникнення нових загроз та небезпек. Так як сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта, то надійне забезпечення інформаційної безпеки стає атрибутом формування клієнтської довіри. Тому, в процесі створення та функціонування бізнесу, задля стійкого розвитку та забезпечення конкурентоспроможності, суб'єктам підприємництва необхідно створити ефективну під систему управління інформаційною безпекою в складі загальної системи управління економічною безпекою підприємства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кавун С. В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навч. посіб. / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. – Харків : Вид. ХНЕУ, 2013. – 364 с.
2. Іванюта Т. М. Економічна безпека підприємства : навч. посіб. / Т. М. Іванюта, А. О. Заїчковський. – Київ : Центр учбової літератури, 2009. – 256 с.
3. Кузенко Т. Б. Фінансова безпека підприємства: навч. посіб. / Т. Б. Кузенко, Л. С. Мартюшева, О. В. Грачов, О. Ю. Литовченко. – Харків: Вид. ХНЕУ, 2010. – 304 с.
4. Отенко І. П. Економічна безпека підприємства : навч. посіб. / Отенко І. П., Іващенко Г. А., Воронков Д. К.– Харків : Вид. ХНЕУ, 2012 – 251 с.

Додаток Б

Анкета

Доброго дня!

Мета опитування – визначення найбільш вагомих ризиків, що можуть виникнути на різних фазах реалізації проекту з впровадження нового виду продукції.

Прошу Вас взяти участь в опитуванні та оцінити кожний з наведених видів ризиків по шкалі від 1 до 10 , де 1 – ризик має найменший негативний вплив на реалізацію бізнес-плану та 10 ризик має найбільший негативний вплив на реалізацію проекту. Укажіть також вагомість окремого ризику.

Таблиця Б.1

Анкета опитування

№	Види проектних ризиків в залежності від фази проекту	Оцінка ризику	Вірогідність ризику
Проектні ризики передінвестиційної фази:			
1	Помилка в прогнозуванні ринків збуту продукції		
2	Помилка у плануванні та проектуванні заходів		
Проектні ризики інвестиційної фази:			
3	Зміна вартості обладнання внаслідок коливань курсу іноземної валюти		
4	Невиконання термінів поставки обладнання		
5	Несправність поставленого обладнання		
6	Відмова постачальників від попередньо укладених контрактів		
Проектні ризики експлуатаційної фази:			
7	Підвищення вартості матеріальних ресурсів		
8	Виробничо-технологічний ризик пов'язаний з недостатністю або якістю робочої сили		
9	Поява нових конкурентів		
10	Виробничо-технологічний ризик пов'язаний з виробничим браком		
11	Вихід з ладу старого обладнання		
12	Зміна податкової політики країни		

Таблиця Б.2

Оцінка ризикованості проекту

№	Види проектних ризиків в залежності від фази проекту	Експерт 1		Експерт 2		Експерт 3	
		Оцінка	Вірогідність	Оцінка	Вірогідність	Оцінка	Вірогідність
Проектні ризики передінвестиційної фази:							
1	Помилка в прогнозуванні ринків збуту продукції	7	0,6	8	0,5	6	0,6
2	Помилка у плануванні та проектуванні заходів	6	0,4	7	0,5	5	0,4
Проектні ризики інвестиційної фази:							
3	Зміна вартості обладнання внаслідок коливань курсу іноземної валюти	7	0,4	8	0,4	6	0,5
4	Невиконання термінів поставки обладнання	5	0,15	6	0,2	5	0,15
5	Несправність поставленого обладнання	5	0,3	5	0,3	6	0,15
6	Відмова постачальників від попередньо укладених контрактів	6	0,15	6	0,1	5	0,2
Проектні ризики експлуатаційної фази:							
7	Підвищення вартості ресурсів	6	0,3	5	0,2	6	0,2
8	Виробничо-технологічний ризик пов'язаний з недостатністю або якістю робочої сили	5	0,1	5	0,15	6	0,15
9	Поява нових конкурентів	6	0,1	7	0,2	7	0,15
10	Виробничо-технологічний ризик пов'язаний з виробничим браком	6	0,2	7	0,15	7	0,25
11	Вихід з ладу старого обладнання	6	0,1	6	0,1	5	0,05
12	Зміна податкової політики країни	7	0,2	6	0,2	6	0,2