

РЕФЕРАТ

Дипломна робота: нараховує 107 сторінок, 42 рисунків, 62 літературне джерело.

Мета дослідження полягає у вивченні теоретичних засад та практичного досвіду підприємства із забезпечення інформаційної безпеки в підприємницькій діяльності та розробці заходів із вдосконалення управління інформаційною безпекою на ТОВ «МІРОПЛАСТ».

Завдання:

- окреслити сутність та основні складові інформаційної безпеки в підприємницькій діяльності;
- охарактеризувати засоби забезпечення інформаційної безпеки;
- розкрити методичні підходи до оцінки інформаційної безпеки підприємства;
- представити загальну характеристику підприємства «ТОВ МІРОПЛАСТ»;
- провести аналіз фінансово-господарського стану ТОВ «МІРОПЛАСТ»; - розглянути організацію системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ»;
- розробити заходи із вдосконалення інформаційною безпекою ТОВ «МІРОПЛАСТ»;
- оцінити ефективність запропонованих заходів.

Об'єктом дослідження є процес організації інформаційної безпеки підприємства.

ЗМІСТ

ВСТУП	6
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПІДПРИЄМНИЦЬКІЙ ДІЯЛЬНОСТІ	9
1.1 Сутність та основні складові інформаційної безпеки в підприємницькій діяльності	9
1.2 Засоби забезпечення інформаційної безпеки	16
1.3 Методичні підходи до оцінки інформаційної безпеки підприємства.....	29
РОЗДІЛ 2 АНАЛІЗ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА «ТОВ МІРОПЛАСТ»	42
2.1 Загальна характеристика підприємства «ТОВ МІРОПЛАСТ»	42
2.2 Аналіз фінансово-господарського стану ТОВ «МІРОПЛАСТ».....	52
2.3 Організація системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ»	65
РОЗДІЛ 3 ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА	79
3.1 Заходи із вдосконалення інформаційною безпекою ТОВ «МІРОПЛАСТ»	79
3.2 Оцінка ефективності запропонованих заходів.....	86
ВИСНОВКИ.....	93
БІБЛІОГРАФІЧНИЙ СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	96
ДОДАТКИ.....	103

ВСТУП

Актуальність теми. Підприємницька діяльність, що здійснюється у різних сферах економіки, нерозривно пов'язана з одержанням і використанням інформації, яка в сучасних умовах розвитку ринкових відносин в економічній сфері, є товаром особливого роду, що має велику значиму цінність. Тому однією з найважливіших проблем розвитку інформаційних технологій на підприємстві є надійне забезпечення інформаційної безпеки.

Управління сучасними вітчизняними підприємствами базується на взаємодії різних систем, серед яких головною, що пускає в хід інші, є інформаційна система. Сьогодні забезпечення інформаційної безпеки підприємницької діяльності є найбільш складним процесом в технології управління, що вимагає особливого ставлення і постійної уваги керівників і власників бізнесу, а також розуміння того, що ефективність процесів управління інформаційною безпекою істотно впливає на ефективність діяльності компанії в цілому. Актуальність загроз цілісності і конфіденційності інформації вимагає уважного ставлення до завдання організації її захисту. Багато проблем інформаційної безпеки пов'язані з недооцінкою важливості такої загрози, як конфіденційність інформації. Помилки в побудові системи інформаційної безпеки підприємств часто обертаються не тільки втратою даних, але і набагато більш серйозними наслідками. В результаті для підприємства це може обернутися банкрутством.

Актуальність дослідження проблеми забезпечення інформаційної безпеки в підприємницькій діяльності визначається загостренням проблем інформаційної безпеки (ІБ) в умовах інтенсивного вдосконалення технологій і інструментів захисту даних та обумовлена необхідністю пошуку нових шляхів підвищення ефективності системи управління інформаційною безпекою на вітчизняних підприємствах.

Вивченням проблеми організації забезпечення інформаційної безпеки в підприємницькій діяльності займалися такі вчені, як: В.М. Абакумов, В.С. Цимбалюк, В.М. Фурашев, С.Ф. Гуцу, Б.А. Кормич, В.С. Цимбалюк, А.І. Марущак, О.В. Герасименко, А.В. Козак, О.А. Сороківська, М.І. Зубок, Є.І. Низенко та ін. Питання інформаційної безпеки підприємства знайшло відображення в наукових працях І.М. Близнюка, В.М. Щербини, В.О. Бондаренко, І.Л. Бучило, Г.В. Козаченко, В.П. Пономарьова та ін.

Незважаючи на велику кількість праць та досліджень у цій сфері, проблема забезпечення інформаційної безпеки в підприємницькій діяльності не втрачає актуальності та потребує подальшої розробки. Аналіз вітчизняного та зарубіжного досвіду переконливо доводить необхідність створення цілісної системи інформаційної безпеки компанії, що погоджує оперативні, оперативно-технічні та організаційні заходи захисту.

Об'єктом дослідження є процес організації інформаційної безпеки підприємства.

Предмет дослідження: теоретичні та практичні аспекти забезпечення інформаційної безпеки в підприємницькій діяльності (на прикладі ТОВ «МІРОПЛАСТ»).

Мета дослідження полягає у вивченні теоретичних засад та практичного досвіду підприємства із забезпечення інформаційної безпеки в підприємницькій діяльності та розробці заходів із вдосконалення управління інформаційною безпекою на ТОВ «МІРОПЛАСТ».

Завдання:

- окреслити сутність та основні складові інформаційної безпеки в підприємницькій діяльності;
- охарактеризувати засоби забезпечення інформаційної безпеки;
- розкрити методичні підходи до оцінки інформаційної безпеки підприємства;
- представити загальну характеристику підприємства «ТОВ МІРОПЛАСТ»;

- провести аналіз фінансово-господарського стану ТОВ «МІРОПЛАСТ»; - розглянути організацію системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ»;
- розробити заходи із вдосконалення інформаційною безпекою ТОВ «МІРОПЛАСТ»;
- оцінити ефективність запропонованих заходів.

Методологічною основою дослідження є сукупність методів і прийомів наукового пізнання. Для вирішення поставлених в роботі завдань були використані наступні методи: теоретичного узагальнення і системного аналізу при дослідженні концептуальних основ інформаційної безпеки підприємницької діяльності та теоретичних аспектів ефективності систем управління інформаційною безпекою підприємства. Для проведення аналізу системи управління інформаційною безпекою підприємства ТОВ «МІРОПЛАСТ» використовувалися: економіко-математичний, структурно-логічний, графічний методи дослідження.

Інформаційну базу дослідження склали законодавчі та нормативно-правові документи Верховної Ради України, Кабінету Міністрів України в галузі забезпечення інформаційної безпеки, публікації вітчизняних і зарубіжних авторів, монографічні дослідження фахівців з інформаційної безпеки, фінансова звітність підприємства.

Практичне значення. Результати дослідження доповнюють знання про роль інформаційної безпеки підприємницької діяльності в підвищенні ефективності діяльності вітчизняних підприємств та можуть слугувати базою для проведення подальших досліджень проблеми. Розроблені заходи щодо підвищення ефективності системи управління інформаційною безпекою підприємства можуть бути застосовані в практичній діяльності підприємств.

Структура роботи. Робота складається з вступу, трьох розділів, висновків, списку використаної літератури та додатків.

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПІДПРИЄМНИЦЬКІЙ ДІЯЛЬНОСТІ

1.1 Сутність та основні складові інформаційної безпеки в підприємницькій діяльності

У сучасному суспільстві інформація є одним із найважливіших стратегічних ресурсів, що забезпечує розвиток в підприємницькій діяльності. Саме тому інформація вимагає особливого захисту. Проблема інформаційної безпеки набуває особливого значення в сучасних умовах широкого застосування автоматизованих інформаційних систем. У зв'язку із зростаючою роллю інформаційних ресурсів у діяльності підприємства, а також внаслідок реальності численних загроз проблема інформаційної безпеки вимагає до себе постійної і значної уваги.

Діяльність будь-якого підприємства залежить від багатьох факторів, що впливають на його економічну безпеку. Зокрема важливим фактором, який впливає на діяльність організації в умовах динамічного розвитку виробництва, є інформаційний [25, с.37]. У системі забезпечення безпеки в підприємницькій діяльності все більшого значення набуває забезпечення інформаційної безпеки підприємства. Це пов'язано із зростаючим об'ємом інформації, що поступає, вдосконаленням засобів її зберігання, передачі та обробки. Переклад значної частини інформації в електронну форму, використання локальних і глобальних мереж створюють якісно нові загрози конфіденційної інформації.

На сьогодні, в науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека» та існує декілька визначень даного феномена.

В роботах В.С. Цимбалюка інформаційна безпека визначається як «... суспільні відносини щодо створення та підтримання на належному (бажаному, можливому) рівні життєдіяльності відповідної інформаційної системи, у тому числі підприємництва» [60, с.88]. Автор характеризує

інформаційну безпеку як стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації. О.А. Сороківська характеризує інформаційну безпеку підприємства як «...суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності» [54, с.32].

В наукових трудах М.Ю. Танцюри зміст інформаційної безпеки полягає в наступному: дане поняття трактується автором як «...відношення рівня інформаційного захисту до рівня інформаційних загроз; сукупність засобів та дій уповноважених осіб спрямованих на захист інформаційних ресурсів та інформаційної інфраструктури даного підприємства в процесі обміну, обробки та зберігання інформації на всіх рівнях інформаційної системи підприємства» [55, с.21].

О.І. Крюковим поняття «інформаційна безпека» характеризується як «...суспільні правовідносини щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації), суспільства і держави безпечних умов їх життєдіяльності; суспільні правовідносини пов'язані з організацією технологій створення, розповсюдження, зберігання та використанням інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави» [38].

С.Ф. Гуцу радить розглядати інформаційну безпеку як «...стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз» [22, с. 35].

Серед головних складових інформаційної безпеки виділяють: обсяг інформаційного продукту; здатність мереж витримувати зростаюче інформаційне навантаження; можливість керувати розвитком вироблення та розповсюдження інформації; можливість доступу до усіх можливих інформаційних джерел, а також відкритість більшості з них.

Слід зазначити, що більшість сучасних дослідників під інформаційною безпекою розуміють єдність трьох складових: забезпечення захисту інформації; захист та контроль національного інформаційного простору; забезпечення належного рівня інформаційної достатності (рис.1.1) [26, с.104].

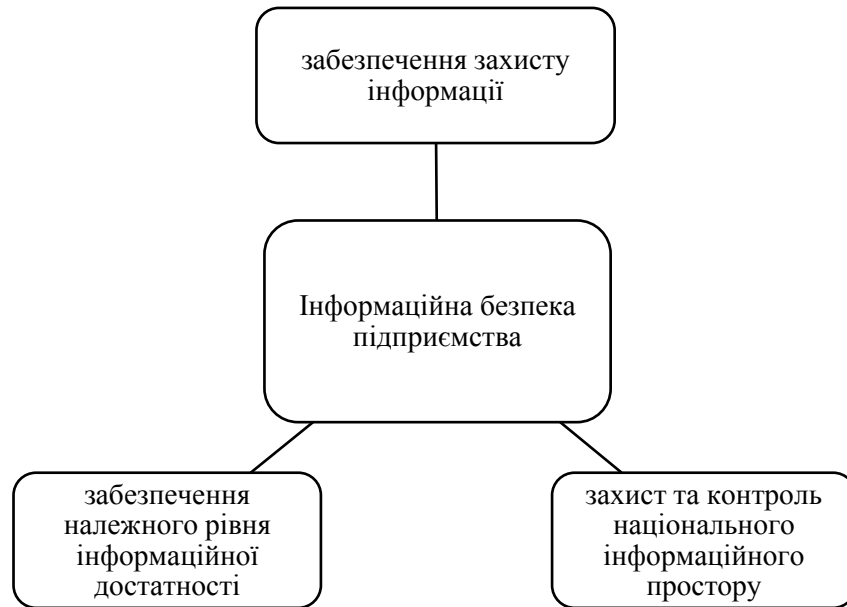


Рисунок 1.1 – Інформаційна безпека підприємства

Інформаційну безпеку підприємницької діяльності умовно можна поділити на наступні підсистеми: комп'ютерна безпека, безпека даних, безпечне програмне забезпечення, безпеку комунікацій (мереж).

До об'єктів інформаційної безпеки організації відносять: інформаційні ресурси, засоби і системи інформатизації, загально-системне і прикладне програмне забезпечення, автоматизовані системи управління підприємством, системи зв'язку і передачі даних, технічні засоби збору, реєстрації, передачі, обробки та відображення інформації[29, с.131].

Результати аналізу наукової літератури свідчать про те, що поняття «інформаційна безпека» розглядається теоретиками та практикаками як в широкому, так і у вузькому сенсі, а основою забезпечення інформаційної безпеки є рішення трьох взаємопов'язаних проблем: захисту інформації, що знаходиться в системі, від впливу внутрішніх та зовнішніх загроз; захисту

інформації від інформаційних загроз; проблема захисту навколишнього середовища від загроз з боку інформації, що знаходиться в системі.

Б.А. Кормич розглядає інформаційну безпеку як «...захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави» [34, с. 241].

Л.С. Харченко, В.А. Ліпкан, О.В. Логінов характеризують інформаційну безпеку як складову національної безпеки, «...процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України» [58, с. 32].

Отже, інформаційна безпека розглядається науковцями як забезпечення реалізації національних інтересів за допомогою різноманітних засобів, що є в її розпорядженні.

Нормативно-правове забезпечення інформаційної безпеки на сьогодні складають: Конституція України, Закони України «Про основи національної безпеки України», «Про інформацію» [1], «Про захист інформації в інформаційно-телекомунікаційних системах» [2] та інші нормативно-правові акти.

Інформаційна безпека підприємства - це набір засобів, методів і робіт, орієнтованих на захист інформаційної інфраструктури підприємства від будь-яких зовнішніх або внутрішніх загроз, які можуть призвести до крадіжки, псування, або несанкціонованого зміни даних на серверах, робочих станціях. Всі роботи орієнтовані на побудову, підтримку і розвиток системи інформаційної безпеки переслідують основну мету - звести до мінімуму можливість заподіяння шкоди інформаційній інфраструктурі підприємства, а в разі форс-мажорних обставин, зведення до мінімуму такого збитку.

Інформаційна безпека (ІБ) підприємства - це стан захищеності корпоративних даних, при якій забезпечується їх конфіденційність,

цілісність, автентичність і доступність[57, с.61]. У системі ІБ повинні враховуватися всі актуальні комп'ютерні загрози і вразливості.

Принципи забезпечення інформаційної безпеки містять в собі: законність, баланс інтересів особи, суспільства і держави; комплексність; системність; інтеграція з міжнародними системами безпеки; економічна ефективність.

О.А. Сороківська характеризує поняття «інформаційна безпека підприємства» як «...суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності» [54, с.34].

В роботах М.Ю. Танцюри інформаційна безпека підприємства розглядається як «...збереження конфіденційності, цілісності та доступності інформації». На думку автора, доступність інформації це властивість бути досяжним та придатним до використання авторизованими сутностями. Цілісність характеризується дослідником як «...властивість захищеності точності та повноти даних, а конфіденційність – як властивість захищеності інформації від неавторизованого використання фізичними особами, сутностями та процесами». Інформаційні активи визначаються як «...знання чи дані, які мають цінність для організації» [55, с. 21].

М.І. Зубок наголошує, що інформаційна безпека підприємства є цілеспрямованою діяльністю структурних підрозділів та посадових осіб організації з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [30, с. 94].

Інформаційна безпека - стан інформаційної обстановки, що характеризується відсутністю небезпеки, надійної захищеністю від загроз і здатністю їх нейтралізувати. Під інформаційною безпекою підприємств слід розуміти загальну захищеність середовища, спрямованої на формування, застосування та розвиток інформації (даних).

Інформаційна безпека організації є цілеспрямованою діяльністю її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток. Здійснюється часто Службою інформаційної безпеки. На нашу думку, інформаційна безпека підприємницької діяльності є комплексним завданням по забезпеченню безпеки і захисту інформації, здійснюване системою безпеки підприємства.

Інформаційна безпека підприємства базується на трьох основних принципах (рис.1.2) [35, с.7]:



Рисунок 1.2 – Основні принципи інформаційної безпеки підприємства

Підкреслимо, що конфіденційність забезпечує доступ до певної інформації, виключно, авторизованим користувачам мережі.

Цілісність даних - це достовірність і повнота інформації, а також, забезпечення її обробки належними методами; результат захисту від збоїв, несанкціонованого створення інформації, її знищення і інших можливих втрат даних.

Доступність інформації реалізується шляхом надання доступу авторизованим користувача до певної інформації.

Принципи забезпечення інформаційної безпеки містять: законність, баланс інтересів особи, суспільства і держави; комплексність; системність; інтеграцію з міжнародними системами безпеки; економічну ефективність.

Конфіденційна інформація, пов'язана з діяльністю конкретної компанії може викликати непідробний інтерес у численних конкурентів, стаючи об'єктом зазіхань. Неналежна увага захисту корпоративних даних здатна привести до фінансових, іміджевих втрат, а також стати причиною банкрутства підприємства. Катастрофічні наслідки може мати незначна недбалість всього лише одного співробітника. Особливий інтерес для зловмисників представляють охоронювані дані, розкрадання і розголошення яких може завдати максимального збитку[38, с.131].

Розглянемо докладніше, з якими загрозами може зіткнутися сучасне підприємство і як може порушуватися його інформаційна безпека. Охарактеризуємо основні види загроз інформаційної безпеки: втрата конфіденційності даних і програм; пошкодження даних; відсутність доступу до інформації; відмова користувача від інформації, що передається; внутрішні загрози (некомпетентність керівництва і співробітників, організація навмисної витоку відомостей).

Загрози класифікуються за природою виникнення (загрози випадкового або навмисного характеру) і по тому, як вони ставляться до захищається (зовнішні і внутрішні загрози).

На рис. 1.3 представлена одна з найбільш популярних класифікацій загроз[39, с.94].

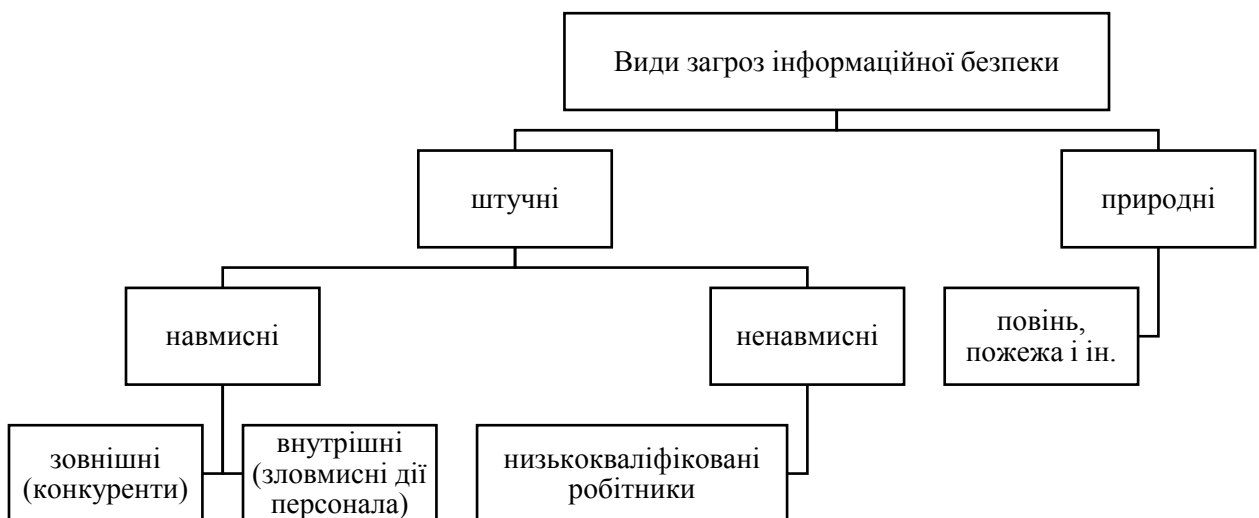


Рисунок 1.3 – Види загроз інформаційної безпеки

Головною метою будь-якої системи інформаційної безпеки є гарантування стійкого функціонування об'єкта, запобігання загрозам його безпеки, захист законних інтересів замовника від протиправних посягань, запобігання розкраданню грошових коштів; розголошуванню, втратам, витоку, спотворенню і знищенню службової інформації; забезпечення нормальної виробничої діяльності всіх підрозділів об'єкта.

О.О. Захаркін серед найпоширеніших видів потенційних загроз безпеці діяльності підприємства у сфері інформаційних технологій виділяє: відсутність регламентованого доступу до файлів даних; вільне втручання в програмне забезпечення; відсутність протоколювання змін у програмному забезпеченні; відсутність регламентації користувачів інформації; відсутність дублювання важливих документів на документальних носіях даних; часті удосконалення одного і того ж програмного забезпечення різними особами; відсутність схем інформаційного забезпечення рівнів управління; наявність непідзвітних посадових осіб у системі управління тощо [28, с.29]

Таким чином, у сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта. Своєю чергою, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємствам необхідно створити ефективну систему управління інформаційною безпекою. Сутність викладеного дає підстави стверджувати, що в сучасних умовах, без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку.

1.2 Засоби забезпечення інформаційної безпеки

Забезпечення інформаційної безпеки (ІБ) є складною і багатогранною проблемою, що повинна вирішуватися всіма економічними агентами і господарюючими суб'єктами. Завдання систем інформаційної безпеки підприємства різноманітні. Це забезпечення захищеного зберігання інформації на різних носіях; захист даних, що передаються по каналах зв'язку; розмежування доступу до різних видів документів; створення резервних копій, після аварійне відновлення інформаційних систем і ін.

Основні умови забезпечення систем інформаційної безпеки підприємницької діяльності спрямовані на виконання певних дій (рис.1.4) [27]:

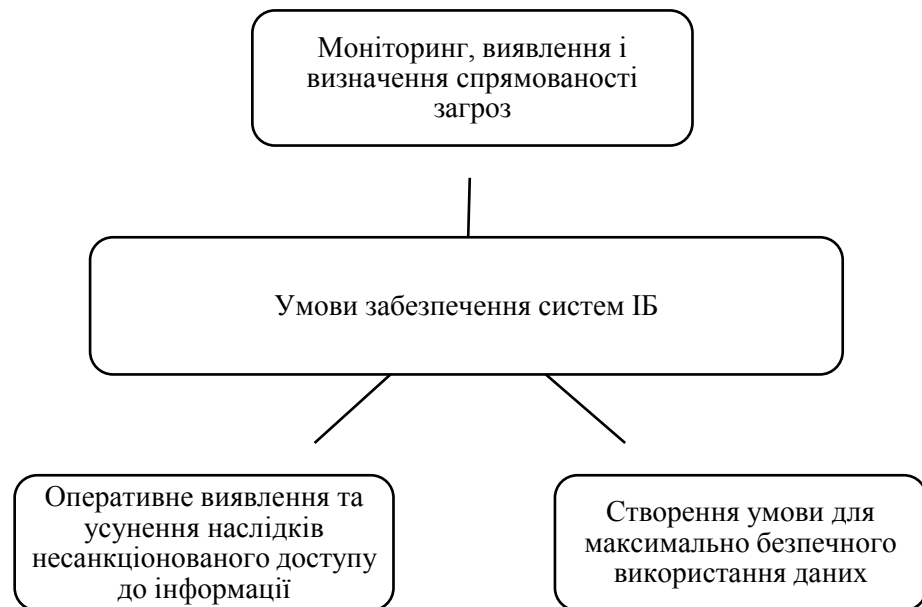


Рисунок 1.4 - Основні умови забезпечення систем ІБ

Забезпечення інформаційної безпеки (ІБ) підприємства можливо тільки при системному і комплексному підході до захисту. В системі ІБ повинні враховуватися всі актуальні комп'ютерні загрози і вразливості. Повноцінна інформаційна безпека підприємств і організацій має на увазі безперервний контроль в реальному часі всіх важливих подій і станів, що впливають на безпеку даних підприємницької діяльності.

На рівні підприємства за інформаційну безпеку відповідають відділи інформаційних технологій, економічної безпеки, кадрів та інші служби [35, с.9].

Захист повинен здійснюватися цілодобово і цілорічно і охоплювати весь життєвий цикл інформації - від її надходження або створення до знищення або втрати актуальності.

Для забезпечення інформаційної безпеки підприємницької діяльності використовують різноманітні засоби і методи захисту інформації. Сучасні засоби і методи захисту інформації спрямовані на захист інформації та даних підприємства, що включають технології запобігають витік інформації і її втрату.

Перешкода	•метод фізичної перешкоди від зловмисника до інформації підприємства, наприклад, металеві двері
Маскування (шифрування)	•захист інформації в каналах зв'язку шляхом її криптографічного шифрування
Регламентація	•метод захисту, заснований на створенні спеціальних умов обробки, зберігання та передачі інформації, при яких можливості несанкціонованого доступу зводяться до мінімуму
Управління	•метод визначення і розподілу інформаційних ресурсів системи авторизованим і санкціонованим користувачам
Пимус	•метод захисту, при якому користувачі та персонал підприємства дотримуються правил обробки, передачі і використання інформації під загрозою матеріальної, адміністративної або кримінальної відповідальності, а обробка інформації регламентуються закріпленими нормативними актами підприємства, держави
Спонування	•створення такої обстановки і умов, при яких правила поведінки з захищеними даними регулюються моральними та етичними нормами

Рисунок 1.5 - Основні методи захисту інформації [37, с.86]

На сьогоднішній день використовуються наступні основні способи захисту інформації (рис.1.5). Перераховані методи мають на меті побудову ефективної технології захисту інформації підприємницької діяльності, при якій виключені втрати через недбалість та успішно відбиваються різні види загроз.

Усі перераховані методи націлені на побудову ефективної технології захисту інформації, при якій виключено витрати через недбалість і успішно відображено різні види загроз.

Система забезпечення інформаційної безпеки наведена на рис.1.6.

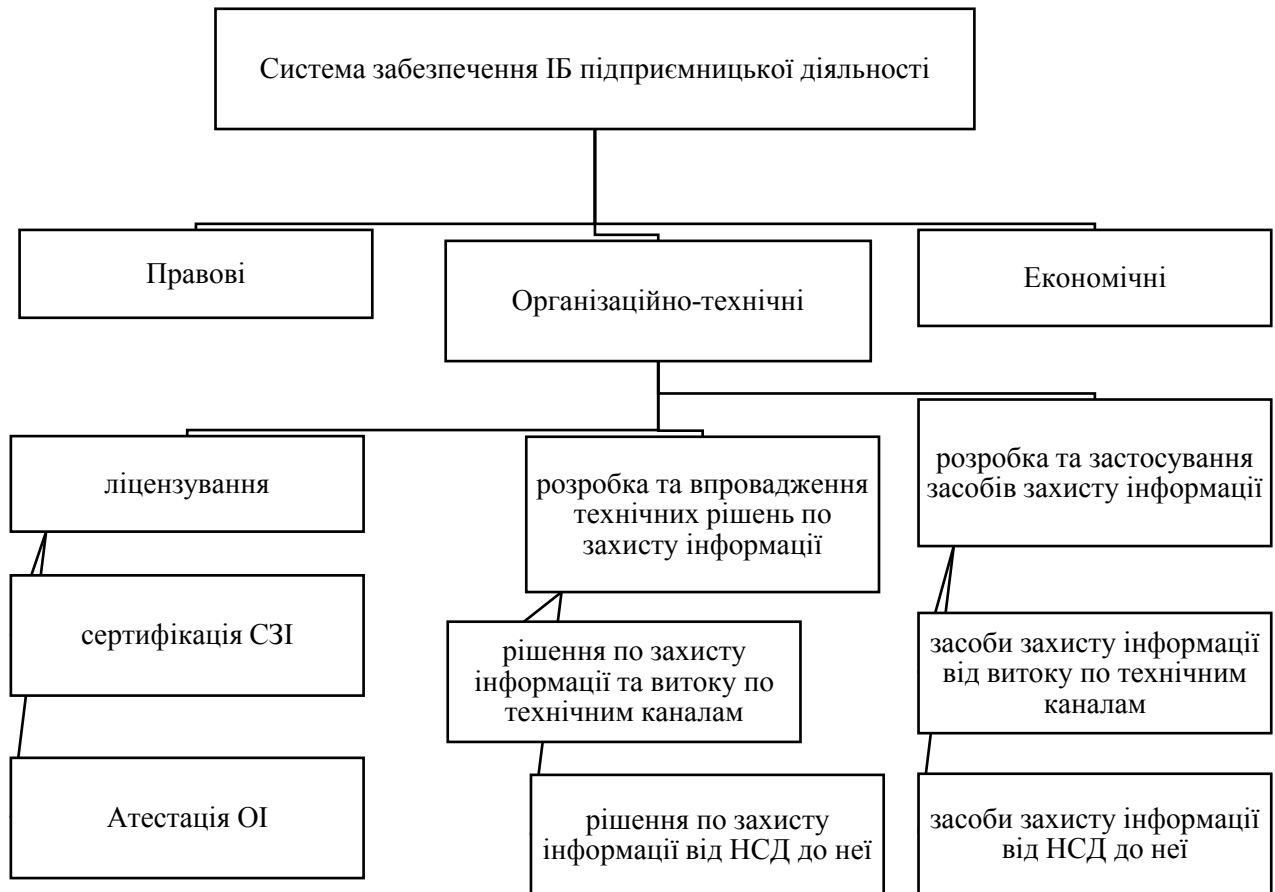


Рисунок 1.6 - Система забезпечення інформаційної безпеки[39, с.94]

Інформаційна безпека підприємства досягається цілим комплексом організаційних і технічних заходів, спрямованих на захист корпоративних даних. За функціональним призначенням методи і засоби інформаційної безпеки можна розділити на такі різновиди: методи і засоби попередження, методи і засоби виявлення, методи і засоби нейтралізації, методи і засоби відновлення.

Якість та ефективність функціонування інформаційної системи визначається рівнем її захищеності від зовнішнього та внутрішнього впливів. Дані світової і вітчизняної статистики свідчать про тенденцію зростання

масштабу комп'ютерних зловживань, що призводять до значних фінансових втрат суб'єктів господарювання різного рівня. Усунення та запобігання інформаційним загрозам різного характеру передбачає побудову чіткої системи діагностики, яка повинна базуватися на оцінці інформаційних ризиків та оцінці зміни економічних, соціальних, техніко-технологічних та інших показників, спричинених зміною стану інформаційної системи підприємства. Існують різні способи захисту інформації та заходи забезпечення інформаційної безпеки, ключовими з яких є програмно-технічні, правові, організаційні, морально-етичні та ін. Перейдемо до розгляду рівнів забезпечення ІБ.

Способи захисту інформації передбачають використання певного набору засобів[41, с.69]:

- фізичні - це засоби захисту реалізуються у вигляді автономних пристроїв і систем: забезпечення безпеки приміщень (пожеже-охоронні системи, системи від збоїв електромережі), засоби забезпечення контролю доступом (СКУД). Вони використовуються для охорони даних як на паперових, так і на електронних носіях;

- програмні і апаратні засоби (технічні).

Під апаратними засобами прийнято розуміти вбудовані технічні пристрої, які використовуються для обробки інформації (схеми контролю інформації по парності, схеми захисту полів пам'яті по ключу і ін.).

До технічних заходів забезпечення безпеки інформації належать засоби авторизації, захисту від несанкціонованого доступу, криптографічні, антивірусні засоби, аналізатори протоколів, системи моніторингу мереж, DLP-системи та інші[45, с.60]. Найбільшою ефективністю відрізняється криптографічний метод захисту, шифрує не тільки канали доступу, але і дані безпосередньо. Багаторівнева система дозволяє використовувати інформацію обмеженого кола осіб. Програмні засоби являють собою програмне забезпечення, призначене для виконання функцій захисту інформації[50, с.16]. Програмні засоби дозволяють здійснювати: реєстрацію та аналіз подій,

що відбуваються в системі; здійснювати контроль цілісності ресурсів системи з метою виявлення моїх модифікацій; шифрування інформації; виконувати захист від зовнішніх вторгнень; здійснювати захист від шкідливого програмного забезпечення (антивірусні пакети, антиспамові фільтри); здійснювати резервне копіювання і відновлення даних. На програмно-технічному рівні здійснюється захист обладнання, програмних засобів та інформаційних ресурсів. Ці заходи засновані на використанні різних пристроїв і спеціальних програм, що входять до складу ІС і виконують (самостійно або в комплексі з іншими засобами) функції захисту з метою усунення загроз, безпосередньо пов'язаних з процесом зберігання, обробки і передачі інформації. Реалізується це за допомогою сервісів безпеки (ідентифікація та аутентифікація; розмежування доступу; протоколювання і аудит; шифрування; екранування, забезпечення цілісності, забезпечення доступності, забезпечення відмовостійкості).

Система аутентифікації являє собою основний метод захисту інформації практично в будь-якій сфері. Зводиться до того, що для отримання доступу до тієї чи іншої інформаційної галузі, консолі управління або каналу зв'язку користувачеві необхідно представити системі свої дані аутентифікації (найчастіше ім'я і пароль). Далі система зіставляє ці дані із заздалегідь визначеною політикою безпеки, після чого надає або не дає користувачеві доступ до запитаної інформації[53, с.72]. Таким чином, кожен користувач в інформаційній структурі має свій особистий ідентифікатор і рівень доступу, що дозволяє йому виконувати будь-які дії тільки в межах цього рівня.

Система шифрування орієнтована на те, що б зловмисник, якому вдалося перехопити певні дані (лист електронної пошти, переносний пристрій зберігання даних і ін.) не міг отримати доступ до них не маючи певного ключа. Існує багато методів шифрування даних, але всі вони діляться на 2 види. Це шифрування із закритим ключем і шифрування з

відкритим ключем. Перше передбачає наявність одного ключа для шифрування і дешифрування даних, друга передбачає наявність двох різних ключів і є найбільш стійким методом.

Міжмережевий екран. Система брандмауера або брандмауер ставить собі за мету відділення локальної мережі конкретного підприємства від глобальної мережі Інтернет. Міжмережевий екран має свою політику безпеки і розмежування доступу, таким чином взаємодія між локальною мережею і глобальною стає можливою тільки в рамках цієї політики.

Віртуальні приватні мережі (VPN). Дана технологія дозволяє передавати дані через глобальні загальнодоступні мережі, такі як Інтернет, через безоплатеві зашифровані VPN тунелі. Таким чином, інформація хоч і передається через глобальну мережу, проте не може бути доступна з неї несанкціоновано.

Фільтрація електронної пошти дозволяє встановлювати певні фільтри на вміст вхідної та вихідної кореспонденції та захищає внутрішню мережу від проникнення небажаних даних, зокрема вірусів, а так само виключаючи витік певних видів інформації з внутрішньої мережі.

Контроль працездатності вузлів орієнтований на постійний моніторинг справності і якості роботи серверів, робочих станцій і мережевого устаткування. Допомогає передбачати і заздалегідь запобігати збоїв в роботі обладнання, які можуть спричинити за собою втрату інформації.

Антивірусний захист орієнтований на запобігання загрозам з боку комп'ютерних вірусів а тісно взаємопов'язаний з фільтрацією електронної пошти і фаєрволом.

Використання систем виявлення слабких місць сприяє виявленню слабких місць в системі захисту інформації шляхом моделювання дій зловмисника і тестування роботи системи при таких діях.

Система резервного копіювання дозволяє зберігати резервні копії певних даних зводячи до мінімуму витрати часу на відновлення даних і робочих процесів після збою.

Технічні заходи засновані на застосуванні різного роду механічних, електро- і електронно-механічних пристроїв і споруд, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів системи і інформації, що захищається, а також засобів візуального спостереження, зв'язку та охоронної сигналізації. Також можна виділити інженерно-технічні заходи, пов'язані з оптимізацією побудови будівель, споруд, мереж інженерних комунікацій, транспортних магістралей і ін., з урахуванням вимог ІБ[59, с.204].

Законодавчі засоби (нормативно-правові) - комплекс нормативно-правових актів, що регулюють діяльність людей, маючих доступ до охоронюваних відомостей і визначають міру відповідальності за втрату або крадіжку секретної інформації[55, с.32].

На концептуально-політичному рівні приймаються документи, що визначають напрями державної політики інформаційної безпеки, формулюються цілі та завдання, шляхи і засоби їх досягнення.

На законодавчому рівні створюється і підтримується комплекс заходів, спрямованих на правове регулювання і забезпечення ІБ, що відображаються в законах та інших правових актах (укази Президента, постанови Уряду та ін.). Найважливішим завданням цього рівня виступає формування механізму, що дозволяє узгодити процес розробки законів з прогресом в області інформаційних технологій.

До правових заходів належать діючі в Україні закони, укази та інші нормативно-правові акти, що регламентують правила поведінки з інформацією та закріплюють права і обов'язки учасників інформаційних відносин в процесі отримання, обробки та використання інформації, а також встановлюють відповідальність за порушення цих правил.

Правові заходи носять в основному попереджувальний, профілактичний характер і вимагають постійної роз'яснювальної роботи з користувачами і обслуговуючим персоналом. Ці заходи в основному

орієнтовані на усунення штучних загроз і є базисом для реалізації інших заходів.

На нормативно-технічному рівні розробляються стандарти, керівні та методичні матеріали, а також інші документи, що регламентують процеси розробки, впровадження та експлуатації засобів забезпечення ІБ. Одним з головних завдань цього рівня є приведення вітчизняних стандартів до міжнародних.

Слід підкреслити на те, що надзвичайно важливим є правовий аспект забезпечення ІБ, пов'язаний з необхідністю вдосконалення законодавчої бази в цій сфері. На сьогоднішній день, нормативно-правова база забезпечення ІБ в Україні не охоплює всього кола проблем в цій галузі, а в окремих питаннях є суперечливою.

Правові заходи інформаційної безпеки, перш за все, включають в себе відповідність всіх заходів щодо захисту інформації з нормативно-методичними документами та законодавчими актами. Ситуація ускладнюється тим, що вітчизняні інформаційні технології відстають від світових стандартів, слабо розвинена вітчизняна індустрія засобів інформатизації, телекомунікацій і зв'язку.

Організаційні заходи відіграють ключову роль в забезпеченні ІБ підприємницької діяльності. Організаційні засоби захисту являють собою організаційно-технічні та організаційно-правові заходи, здійснювані в процесі створення і експлуатації спеціального ПО і апаратних пристроїв для забезпечення захисту інформації підприємницької діяльності[50, с.15].

На рівні організації (підприємства) здійснюються конкретні заходи щодо забезпечення ІБ. Їх склад і зміст визначаються особливостями конкретної організації або підприємства. В основі подібних заходів лежить політика ІБ організації, що представляє собою сукупність документованих управлінських рішень, метою яких є забезпечення захисту інформації та пов'язаних з нею ресурсів, які визначають стратегію, необхідну кількість

коштів і ресурсів, що виділяються організацією на забезпечення належної ІБ підприємницької діяльності.

Політика ІБ формується на основі проведення аналізу існуючих ризиків, що загрожують інформаційній системі підприємства.

До організаційних належать заходи адміністративного та процедурного характеру, які регламентують процеси функціонування ІС, використання її ресурсів, діяльність обслуговуючого персоналу, а також порядок взаємодії користувачів і обслуговуючого персоналу з ІС таким чином, щоб найбільшою мірою утруднити чи унеможливити реалізації загроз безпеці або знизити розмір втрат в разі їх реалізації. Сюди ж слід віднести процедури (механізми) прийняття рішень з управління ІБ, і в першу чергу - механізми розподілу ресурсів, що виділяються на заходи з підтримки та підвищення ІБ підприємницької діяльності. На процедурному рівні визначаються безпосередні заходи щодо забезпечення ІБ, здійснювані людьми. До них відносяться: управління персоналом, фізичний захист і планування відновлювальних робіт.

Організаційні заходи - це єдине, що залишається, коли інші методи і засоби захисту відсутні або не можуть забезпечити підприємству необхідний рівень ІБ. Організаційні заходи необхідні для ефективного застосування інших заходів в частині, що стосується регламентації діяльності людей [37, с.84]. У той же час організаційні заходи необхідно підтримувати економічними, інженерно-технічними, технічними та програмно-апаратними засобами. До організаційних заходів забезпечення інформаційної безпеки підприємницької діяльності належить встановлення політики безпеки підприємства.

Морально-етичні (психологічні засоби) - комплекс заходів для створення особистої зацікавленості працівників у збереженні та автентичності інформації.

Створюючи системи захисту інформаційної безпеки підприємницької діяльності на підприємстві, необхідно враховувати, що, по-перше, для

ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різноманітних заходів, які можна розподілити на три групи: юридичні, організаційно-економічні й технологічні[34, с.101].

По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту.

Аналіз поглядів і концептуальних підходів до формування сучасних ефективних систем інформаційної безпеки підприємства дозволив сформулювати основні функції та завдання і намітити організаційні основи функціонування відповідних підрозділів інформаційної безпеки. У сучасному поданні рольових функцій служби інформаційної безпеки можна виділити чотири напрями [13, с. 85]:

- розробка методології та методики аналізу загроз, оцінки рівня інформаційної безпеки підприємства і системи її забезпечення;
- організація і здійснення конкретних видів діяльності із захисту інформації;
- експлуатація технічних засобів захисту інформації;
- аудит і контроль функціонування системи інформаційної безпеки підприємства.

Таким чином, на сьогодні існує безліч способів боротьби з загрозами інформаційній безпеці підприємницької діяльності.

Для кожної загрози підбираються свої методи і процеси, які контролюють певні вузли інформаційної системи і запобігають будь-якому збою в них. Однак максимального ефекту можна домогтися тільки застосуванням всіх цих методів в комплексі. Тобто проектування, побудова, впровадження і підтримка системи інформаційної безпеки - це комплексна

задача, яка потребує аналізу потенційних загроз, вибору методів боротьби з ними та налагодження взаємодії між цими методами.

Інформаційна безпека є одним з головних умов нормальної роботи і розвитку інформаційної системи будь-якого підприємства, а так само допомагає звести до мінімуму можливість витоку інформації.

Автоматизація доступу і робочих процесів - перше, що необхідно зробити з метою забезпечення інформаційної безпеки підприємства. Для цього використовується цілий комплекс систем, що здійснюють захист даних, що знаходяться на електронних носіях від несанкціонованого використання і впливу вірусів. Найважливішими опціями спеціалізованих систем є: створення резервних копій і відновлення пошкоджених даних[15, с.108].

Слід зазначити, що повноцінний захист неможливий без цілодобового контролю за інформацією, який повинен здійснюватися до того моменту, поки дані не втратять актуальність або не будуть повністю вилучені.

При установці системи автоматизації та захисту необхідно враховувати її функціональне призначення і економічну ефективність, що дозволить підібрати оптимальне обладнання та програмне забезпечення. Активно використовуватися в забезпеченні інформаційної безпеки повинні інтернет-ресурси, засоби і рішення, розробники яких здатні запропонувати ефективні та доступні онлайн-сервіси.

Система інформаційної безпеки підприємства повинна бути максимально технологічною, здатною ефективно протистояти загрозам усіх типів. Тільки так вона зможе стати надійним захистом для інформаційного середовища підприємства.

Розробка якісного багаторівневого захисту має на меті облік видів, форм і способів виникнення можливих загроз[25, с.103].

1.3 Методичні підходи до оцінки інформаційної безпеки підприємства

Усунення та запобігання інформаційним загрозам різного характеру передбачає побудову чіткої системи оцінки інформаційної безпеки, яка повинна базуватися на оцінці інформаційних ризиків та оцінці зміни економічних, соціальних, техніко-технологічних та інших показників, спричинених зміною стану інформаційної системи підприємства.

Критерії оцінки ІБ - це все те, що дозволяє встановити значення оцінки для об'єкта оцінки. В якості критеріїв оцінки ІБ можуть використовуватися вимоги до ІБ, процедури ІБ, поєднання вимог і процедур ІБ, рівень інвестицій, витрати на ІБ.

Контекст оцінки інформаційної безпеки підприємства об'єднує цілі і призначення оцінки ІБ, вид оцінки (незалежна оцінка, самооцінка), об'єкт і області оцінки ІБ, обмеження оцінки і ролі, а модель оцінки ІБ визначає сферу оцінки, що відображає контекст оцінки ІБ в рамках критерію оцінки ІБ, відображення і перетворення оцінки в параметри об'єкта оцінки, а також встановлює показники, що забезпечують оцінку ІБ.

Слід зазначити, що концептуальні основи оцінки інформаційної безпеки виникли ще в 70-х рр., при формуванні моделі безпеки з повним перекриттям (моделі Клементса-Хоффмана) [40]. У своєму первісному вигляді модель Клементса-Хоффмана була «ідеалізована», проте саме в процесі аналізу даної моделі і виникла проблема необхідності оцінки інформаційних загроз.

Модель побудована виходячи з постулату, що система інформаційної безпеки повинна мати, принаймні, один засіб для забезпечення безпеки на кожному можливому шляху впливу порушника на інформаційну систему. Для опису системи захисту інформації з повним перекриттям розглядаються три підмножини [14]:

- множина загроз: $U = \{U_i\}$, $i = 1, m$; множина об'єктів захисту $O = \{O_j\}$, $j=1, n$;

- множина механізмів захисту $M = \{M_k\}$, $k = 1, r$.

Елементи множин U і O знаходяться між собою у відносинах «загроза – об’єкт». Дуга множина $\langle U_i, O_j \rangle$ існує тоді, коли U_i – засіб отримання доступу до об’єкта O_j .

Сучасні погляди на оцінку рівня інформаційної безпеки мають іншу спрямованість на відміну від основоположних концепцій. Так, в роботах Н.Й. Реверчук, О.В. Рибальського пропонується використовувати такі показники інформаційної безпеки підприємства як: продуктивність інформації, коефіцієнт інформаційної озброєності та коефіцієнт захищеності інформації [51, с. 78]. Дані показники відображають лише фінансовий аспект інформаційної безпеки, оскільки в якості вихідних даних для розрахунку зазначених показників виступають витрати на придбання інформаційних ресурсів.

М.Ю. Журавель, С.М. Ілляшенко пропонує оцінювати рівень інформаційної безпеки як частку неповної, неточної і суперечливої інформації, яка використовується в процесі прийняття управлінських рішень, тобто надає оцінку лише якості інформації, що надається особам, які приймають рішення [27, с. 175].

У загальному вигляді процес проведення оцінки ІБ представлений основними компонентами процесу: контекст, свідоцтва, критерії та модель оцінки, що є необхідними для реалізації процесу оцінки.

Оцінка ІБ полягає у виробленні оціночного судження щодо придатності (зрілості) процесів забезпечення ІБ, адекватності використовуваних захисних заходів або доцільності (достатності) інвестицій для забезпечення необхідного рівня ІБ на основі вимірювання і оцінювання критичних елементів (факторів) об’єкта оцінки.

Залежно від обраного для оцінки інформаційної безпеки критерію В.В. Андріанов розділяє способи оцінки інформаційної безпеки підприємства на оцінку за еталоном, ризик-орієнтовану оцінку та оцінку за економічними показниками (рис.1.7) [10, с. 186].



Рисунок 1.7 - Способи оцінки ІБ підприємства

Спосіб оцінки ІБ за еталоном зводиться до порівняння діяльності та заходів щодо забезпечення ІБ організації з вимогами, закріпленими в еталоні. По суті справи проводиться оцінка відповідності ІБ організації встановленому зразку. Під оцінкою відповідності ІБ організації згідно встановленим критеріям розуміється діяльність, пов'язана з прямим або непрямим визначенням виконання або невиконання відповідних вимог ІБ в організації. За допомогою оцінки відповідності ІБ вимірюється правильність реалізації процесів системи забезпечення ІБ організації та ідентифікуються недоліки такої реалізації.

В результаті проведення оцінки ІБ повинна бути сформована оцінка ступеня відповідності ІБ еталону, в якості якого можуть бути прийняті:

- вимоги законодавства в області ІБ;
- галузеві вимоги щодо забезпечення ІБ;
- вимоги нормативних, методичних та організаційно-розпорядчих документів щодо забезпечення ІБ;
- вимоги національних і міжнародних стандартів в області ІБ.

Основні етапи оцінки інформаційної безпеки за еталоном включають: вибір еталона і формування на його основі критеріїв оцінки ІБ, збір свідчень оцінки і вимірювання критичних елементів (факторів) об'єкта оцінки, формування оцінки ІБ.

Ризик-орієнтована оцінка ІБ організації являє собою спосіб оцінки, при якій розглядаються ризики ІБ, що виникають в інформаційній сфері організації, і зіставляються існуючі ризики ІБ та вжиті заходи по їх обробці. В результаті повинна бути сформована оцінка здатності організації ефективно управляти ризиками ІБ для досягнення своїх цілей.

Основні етапи ризик-орієнтованої оцінки інформаційної безпеки включають ідентифікацію ризиків ІБ, визначення адекватних процесів управління ризиками і ключових індикаторів ризиків ІБ, формування на їх основі критеріїв оцінки ІБ, збір свідчень оцінки і вимірювання ризик-факторів, формування оцінки ІБ.

Спосіб оцінки ІБ на основі економічних показників оперує зрозумілими для бізнесу аргументами про необхідність забезпечення та вдосконалення ІБ. Для проведення оцінки в якості критеріїв ефективності ІБ використовуються показники сукупної вартості володіння (Total Cost of Ownership - TCO) [13, с. 30].

Під показником TCO розуміється сума прямих і непрямих витрат на впровадження, експлуатацію та супровід СОІБ. Під прямими витратами розуміються всі матеріальні витрати: покупка обладнання і програмного забезпечення, трудовитрати відповідних категорій співробітників. Непрямими є всі витрати на обслуговування СОІБ, а також втрати від інцидентів. Збір і аналіз статистики по структурі прямих і непрямих витрат проводиться, як правило, протягом року. Отримані дані оцінюються по ряду критеріїв з показниками TCO аналогічних організацій галузі. Оцінка на основі показника TCO дозволяє оцінити витрати на інформаційну безпеку і порівняти ІБ організації з типовим профілем захисту, а також надає змогу управляти витратами для досягнення необхідного рівня захищеності.

Основні етапи оцінки ефективності СОІБ на основі моделі TCO включають збір даних про поточний рівень TCO, аналіз областей забезпечення ІБ, вибір порівнянної моделі TCO як критерій оцінки, порівняння показників з критерієм оцінки, формування оцінки ІБ.

В роботах О.Я. Кравчука для оцінки рівня інформаційної безпеки пропонується розрахування п'ять показників, що характеризують рівень інформаційно-аналітичного супроводження діяльності підприємства, захисту комерційної інформації та безпеки документообігу, рівень ділової репутації та іміджу продукції [37, с.26].

Шляхом поєднання вищезазначених методичних підходів до оцінки рівня інформаційної безпеки М.Ю. Журавель, Т.В. Полозова та ін. запропонували проводити діагностику рівня інформаційної безпеки підприємства за трьома ключовими напрямками: оцінка програмно-технічної захищеності інформації, оцінка інформаційної надійності персоналу, оцінка інформації, що надається особам, що приймають рішення, інформаційною службою підприємства [27, с. 176].

В дослідженні А.В. Велігури до оцінки рівня інформаційної безпеки підприємства запропоновано використання трьох основних показників[14, с. 159]:

- 1 оцінка небезпек, з якими стикається підприємство. Шляхом оцінки небезпек визначаються загрози для інформації, її вразливість та ймовірність виникнення загроз, а також можливий збиток.

- 2 – це законодавчі, нормативні та договірні вимоги, які повинна дотримуватися організація, її партнери по бізнесу, підрядники та постачальники послуг.

- 3 – певний набір принципів, цілей і вимог до обробки інформації, розроблених організацією для підтримки своєї діяльності. Визначення вимог до безпеки проводиться шляхом методичної оцінки ризиків. Витрати на підтримку безпеки необхідно збалансувати з шкодою для бізнесу, який може виникнути при порушенні безпеки [6].

Серед методів оцінки рівня ІБ за виділеними критеріями більшість авторів пропонують використовувати метод експертної оцінки.

Метод експертних оцінок - це прадавній науковий метод, який дозволяє отримати об'єктивну оцінку на основі певної сукупності індивідуальних думок експертів. Для розрахунку узагальненої думки здійснюється розрахунок середніх величин. Якщо склад експертів однорідний, то розраховується проста середня арифметична (М) (1.1) [30, с. 102]:

$$M = \Sigma V / N, \quad (1.1)$$

де V - індивідуальна думка кожного експерта; Σ - знак суми; n - кількість експертів.

Якщо ж склад експертів є неоднорідним (як при проведенні нашої експертної оцінки), то з-поміж експертної групи визначаються провідні фахівці, думка яких стосовно певних питань є більш значимою. Кожному з експертів у таких випадках присвоюється ваговий коефіцієнт (К). При опрацюванні результатів експертної оцінки на прикладі впровадження системи моніторингу стану здоров'я населення на рівні первинної медико-санітарної допомоги було використано шкалу ваги експертів.

Для встановлення переліку критеріїв оцінювання стану інформаційної безпеки, спочатку визначають групи суб'єктів зовнішнього та внутрішнього середовищ, від гармонізації інтересів яких залежить інформаційна безпека підприємства.

Слід зазначити, що метод експертних оцінок, в якому зараз широко застосовується апарат математичної статистики, використовується для обробки результатів експертного аналізу. Методи регресійного і дисперсійного аналізу застосовуються для встановлення зв'язків між окремими показниками інформаційної безпеки. У результаті багатофакторного кореляційно-регресійного аналізу встановлюються фактори, що впливають на інформаційну безпеку підприємства, та будується адекватна і великою мірою достовірна економіко-математична модель, яка описує зв'язок між інтегральним показником інформаційної безпеки та встановленими формалізованими факторами. Також ряд авторів звертають

увагу на доцільності використання методу критичних сценаріїв, коли в сценаріях аналізуються ситуації, як уявний злочинець наносить шкоди інформаційній системі підприємства і відповідно знижує здатність підтримувати управління в межах оптимальних параметрів [26, с. 151].

Далі розглянемо методику оцінки можливості (оцінки зрілості) процесів для оцінки ІБ організації. В ISO / IEC 15504 визначена модель оцінки зрілості процесів менеджменту ІБ організації ISF (Information Security Forum). Дана модель визначає шість рівнів зрілості організації - з нульового по п'ятий. Основу моделі складають ідентифіковані атрибути оцінюваних процесів, що представляють вимірні характеристики можливостей того чи іншого процесу, і методи їх оцінювання. Стандартом визначена наступна шкала рейтингів оцінки процесу, що визначають ступінь досягнення певних значень для оцінюваного атрибуту процесу[65, с. 304]:

- N - не досягнуто;
- P - частково досягнуто. Існують деякі свідчення наближення до бажаного значення певного атрибуту оцінюваного процесу;
- L - в значній мірі досягнуто. Існують свідчення систематичного наближення до певного значення атрибуту оцінюваного процесу;
- F - повністю досягнуто. Існують свідчення повного і систематичного наближення до певного значення атрибуту оцінюваного процесу.

Фактично розглядаються певні показники атрибутів процесів, які ранжуються за чотирьох рівневою шкалою оцінювання. Значення для оцінюваних параметрів визначені наступні:

- N - «не досягнуто - від 0 до 15%;
- P - «частково досягнуто» - від > 15 до 50%;
- L - «в значній мірі досягнуто» - від > 50 до 85%;
- F - «повністю досягнуто» - від > 85 до 100%.

При цьому будь-яка інформація, що підлягає дослідженню та оцінюванню, представлена в специфікації процесного підходу згідно виділених атрибутів даного процесу і встановлених методів вимірювання.

Для оцінки ІБ на основі моделі зрілості необхідні наступні два основних джерела:

- вимоги до складу процесів менеджменту ІБ організації - вимоги стандарту ISO / IEC 15504, ДСТУ Р 27001;
- еталонна модель зрілості процесів ІБ.

Для ідентифікованих процесів забезпечення ІБ повинні бути розроблені:

- опис кожного з процесів в термінах рівнів зрілості еталонної моделі;
- методика оцінки зрілості процесів, що включає анкети для оцінки можливостей процесів, відповідно до заявленого рівнем зрілості.

Оцінка поточного стану системи ІБ порівнює вибудовану по вже існуючому стандарту «ідеальну» модель вимог ІБ з тими, що вже були реалізовані в компанії у вигляді поточних захисних заходів. Її результати легко зрозуміти і побачити певні слабкі місця.

Узагальнюючи форми, методи та підходи доцільно запропонувати групи показників оцінки інформаційної безпеки, які базується на основних напрямках захисту інформації та враховують: оцінку програмно-технічної захищеності інформації, оцінку витрат на забезпечення інформаційної безпеки, оцінку інформаційної надійності персоналу, оцінку інформації, що надається особам, які приймають рішення, інформаційною службою підприємства, оцінка ризику, надійності, гнучкості та керованості системи захисту інформації Д.В. Дячков розробив наступну методику оцінки ІБ (табл. 1.1) [24, с. 38]. Особливістю пропонованої автором системи показників оцінки інформаційної безпеки підприємства є те, що вона охоплює економічні показники, технічні та програмні параметри системи інформаційної безпеки та надає оцінку персоналу, який здійснює управління зазначеною підсистемою. Також така система показників оцінки інформаційної безпеки підприємства може бути застосована на будь-кому підприємстві, не залежно від його розміру, сфери та напрямку діяльності, що робить її універсальною. Водночас, варто зазначити, що в залежності від

мети діагностики рівня інформаційної безпеки показники в кожній групі можуть бути доповнені або замінені.

Таблиця 1.1 - Показники оцінки інформаційної безпеки підприємства (Д.В. Дячков)

№	Показники ІБ	Характеристика
1	2	3
Оцінка програмно-технічної захищеності інформації		
1	Коефіцієнт фінансування технічної захищеності інформації	Співвідношення вартості технічного забезпечення, яке застосовується для створення інформаційного захисту до загальних витрат на інформаційну безпеку
2	Коефіцієнт технічного захисту інформації	Співвідношення кількості відвернутих інформаційних атак до загальної кількості інформаційних атак за певний проміжок часу.
3	Коефіцієнт програмної захищеності інформації	Співвідношення часу безперебійного функціонування корпоративної інформаційної системи до нормативного часу функціонування корпоративної інформаційної системи.
4	Коефіцієнт фінансування програмно-технічної захищеності інформації	Співвідношення витрат на програмно-технічний захист інформаційних ресурсів до витрат на придбання інформаційних ресурсів.
5	Коефіцієнт фінансування інформаційних служб підприємства	Співвідношення витрат утримання інформаційної служби підприємства до загальних витрат підприємства.
6	Коефіцієнт автоматизації програмно-технічної захищеності інформації	Співвідношення автоматизованих процесів спрямованих на програмно-технічний захист інформації до загальної кількості процесів спрямованих на програмно-технічний захист інформації
Оцінка витрат на забезпечення інформаційної безпеки		
7	Коефіцієнт фінансування інформаційної безпеки	Співвідношення витрат на забезпечення інформаційної безпеки підприємства до загальних витрат підприємства.
8	Коефіцієнт фінансування інформаційної безпеки, що забезпечує фінансовий	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фінансового напрямку діяльності підприємства до витрат на забезпечення інформаційної
9	Коефіцієнт фінансування інформаційної безпеки, що забезпечує фізичний захист	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист фізичних об'єктів підприємства до витрат на забезпечення інформаційної підприємства.
10	Коефіцієнт фінансування інформаційної безпеки, що забезпечує захист	Співвідношення витрат на забезпечення інформаційної безпеки, яка спрямована на захист персоналу підприємства до витрат на забезпечення інформаційної підприємства.
Оцінка інформаційної надійності персоналу		
11	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку	Співвідношення чисельності працівників, маючих доступ до комерційної таємниці (баз даних, банків даних тощо), що працюють на підприємстві більше одного року до загальної чисельності
12	Коефіцієнт надійності персоналу, що забезпечує інформаційну	Співвідношення чисельності працівників, звільнених за причиною витоку інформації до загальної чисельності звільнених працівників.
13	Коефіцієнт підготовленості персоналу до розпізнавання загроз інформаційній	Співвідношення чисельності, ненавмисні дії яких призвели до витоку інформації через низький рівень компетентності персоналу та невміння розпізнавання загроз інформаційній безпеці до
14	Коефіцієнт правової захищеності інформації	Співвідношення обсягу інформації, розголошення якої може спричинити негативні наслідки для підприємства до загального обсягу юридично захищеної інформації.

15	Коефіцієнт компетентності персоналу, який забезпечує інформаційну безпеку	Співвідношення інформаційних загроз (інформаційних атак), які відвернуті через дії персоналу, який забезпечує інформаційну безпеку до загальної кількості інформаційних атак за певний
----	---	--

Продовження таблиці 1.1

	Оцінка інформації, що надається особам, які приймають рішення, інформаційною службою підприємства	
№	Показники ІБ	Характеристика
16	Коефіцієнт повноти інформації	Співвідношення обсягу інформації, що є в розпорядженні ОПР до обсягу інформації, необхідної для ухвалення обґрунтованого рішення.
17	Коефіцієнт точності інформації	Співвідношення обсягу релевантної інформації до загального обсягу наявної в розпорядженні ОПР інформації.
18	Коефіцієнт суперечливості інформації	Співвідношення кількості незалежних свідчень на користь ухвалення рішення до загальної кількості незалежних свідчень у сумарному обсязі релевантної інформації.
19	Коефіцієнт своєчасності надання інформації	Співвідношення обсягу своєчасно наданої ОПР інформації до обсягу інформації, необхідної для ухвалення обґрунтованого рішення.
20	Коефіцієнт надійності інформації	Співвідношення обсягу інформації, наданої ОПР з перевірених джерел до загального обсягу наданої ОПР
	Оцінка системи захисту інформації	
21	Ступінь інформаційного ризику	відсоток втрат (у грошову вираженні) спричинених пошкодженням інформаційної цілісності
22	Гнучкість системи інформаційної безпеки підприємства	Здатність системи управління інформаційною безпекою швидко адаптувати організаційну побудову до зовнішніх та внутрішніх потреб.
23	Коефіцієнт керованості системи інформаційної безпеки підприємства	Співвідношення компетентностей керівного персоналу системи інформаційної безпеки до загальних компетентностей, якими повинен володіти керівник відповідного рівня.
24	Частка програмного забезпечення, розробленого працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства.	
25	Частка технічних засобів, розроблених працівниками підприємства, яке задіяне для забезпечення інформаційної безпеки підприємства.	

Також заслуговує уваги методика оцінки ІБ ранжуванням інформації за рівнями важливості. На основі списку ідентифікованої інформації, що захищається експертна комісія визначає важливість збереження властивостей кожного інформаційного ресурсу для організації і безпосередню його цінність. В рамках запропонованої методики можна використовувати будь-яку кількісну оцінку важливості - як базову з рангами: 1 - «неважлива», 2 - «важлива», 3 - «критично важлива» і ін. Способи оцінки важливості інформації і її властивостей в своїх роботах пропонували В.С. Ходаков, А.Ф. Чипига, І.Ю. Нежданов та ін.

В результаті проведеного аналізу науково-методологічної літератури нами було розроблено блок-схему процесу оцінювання рівня інформаційної безпеки підприємства (рис. 1.8)



Рисунок 1.8 - Процес оцінювання рівня інформаційної безпеки підприємства

На рис. 1.8 наведено узагальнену блок-схему процесу оцінювання рівня інформаційної безпеки підприємства; при цьому деталізація не доведена до

малозначних операцій. У блок-схемі показано різні випадки здійснення процесу оцінювання. Входи елементів (операцій) Еі схеми позначені символами x_i (вхідна інформація); виходи – y_i (результати опрацювання вхідної інформації).

До позитивних особливостей моделі можна віднести такі: за основу прийнято ряд незаперечних положень найдосконаліших методик оцінювання рівня ІБ підприємств; оцінювання повинно здійснюватися як за окремими індикаторами, функціональними складовими ІБ підприємства, рівнями оцінки (тактичним та стратегічним), так і передбачати розрахунок інтегрального показника; за кожним із визначених рівнів можна чітко ідентифікувати ступінь безпеки, тобто є можливість як аналізу, так і синтезу з метою виявлення впливу ключових факторів на підготовку оптимальних управлінських рішень; необхідність систематичного коригування методичних засад оцінки рівня безпеки реалізована через етап «адаптації», який забезпечує виявлення проблемних сфер і коригування методики.

Для оцінки реального стану ІБ підприємства можуть застосовуватися різні критерії. Аналіз вітчизняного й закордонного досвіду показав спільність підходів до визначення стану інформаційної безпеки у різних країнах. Для можливості оцінки вводиться деяка система показників і задається ієрархія класів безпеки. Кожному класу відповідає певна сукупність обов'язкових функцій. Ступінь реалізації обраних критеріїв показує поточний стан інформаційної безпеки. Наступні дії зводяться до порівняння реальних загроз із реальним станом безпеки. Якщо реальний стан перекриває загрози повною мірою, система безпеки вважається надійною й не вимагає додаткових заходів. Таку систему можна віднести до класу систем з повним перекриттям загроз і каналів витоку інформації. Інакше система інформаційної безпеки має потребу в додаткових заходах захисту.

Е.І. Низенко, В.Г. Алькема, М.І. Копитко розглядають інформаційну безпеку як частину економічної безпеки підприємства і виділяють наступну

сукупність індикаторів та їхні граничні значення для оцінки рівня інформаційної безпеки підприємства (табл.1.2) [47, с. 75]

Таблиця 1.2 - Сукупність індикаторів та їхні граничні значення для оцінки рівня інформаційної безпеки підприємства

Показник	Алгоритм для розрахунку	Граничне значення	Оцінка рівня ІБ
1	2	3	4
Рівень забезпечення працівників інформацією для прийняття рішень	Визначається вербально експертним шляхом	високий	високий – (0,7-1,0)
		середній	достатній – (0,35-0,7)
		низький	низький – (0-0,35)
Рівень захисту комерційної інформації	Відношення збитків через втрату комерційної інформації до загальної суми витрат підприємства	< 1	високий – (0,7-1,0)
		1-3	достатній – (0,35-0,7)
		> 3,0	низький – (0-0,35)

Авторами запропоновано характеризувати рівень інформаційної безпеки за трьома рівнями:

- низький – фактичне значення окремого індикатора, функціональної складової, рівня оцінки чи інтегрального показника характеризується наявністю тенденцій зростання рівня небезпеки, фактичних ознак кризи та загрози існуванню підприємства як соціально-економічної системи;
- достатній – фактичне значення перебуває в допустимих межах, коли рівень інформаційної безпеки уможливорює функціонування підприємства, хоча рівень безпеки є недостатньо високим, існує можливість реалізації окремих загроз і зростання рівня небезпеки в майбутньому;
- високий – розраховане фактичне значення вказує на високий рівень інформаційної безпеки, стійкість і можливість розвитку підприємства як соціально-економічної системи.

Отже, проведений аналіз дозволив визначити два основних підходи до оцінки інформаційної безпеки підприємства: перший заснований на характеристиці захисних для об'єкта оцінки механізмів і достатності системи захисту; другий підхід заснований на тісному зв'язку системи показників кількісних оцінок інформаційної безпеки з ефективністю функціонування

інформаційної системи в умовах впливу всіх видів загроз інформаційної безпеки.

РОЗДІЛ 2 АНАЛІЗ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА «ТОВ МІРОПЛАСТ»

2.1 Загальна характеристика підприємства «ТОВ МІРОПЛАСТ»

Українська компанія ТОВ «МІРОПЛАСТ» є лідером ринку ПВХ-профілю в Україні, який постійно нарощує свої виробничі потужності. Профільні системи ПВХ дозволяють створювати функціональні та естетичні вікна та двері для дому, офісу, комерційних та виробничих приміщень, забезпечуючи безпеку та відмінну звуко- та теплоізоляцію.

ТОВ «МІРОПЛАСТ» є компанією приватної власності, що має статус юридичної особи. Адреса ТОВ «МІРОПЛАСТ»: 49051, Україна, Дніпро, вул. Курсантська, 10. Код ЄГРПОУ 34230288.

Основними цінностями ТОВ «МІРОПЛАСТ» є: задоволення потреб споживача; виконання зобов'язань; персональний розвиток; взаємна підтримка.

Стратегія компанії: збільшення прибутків компанії та зміцнення позиції на ринку, подальше зростання та розвиток в обраних категоріях бізнесу і регіонах.

ТОВ «МІРОПЛАСТ» почало свою роботу у 2006 році після завершення будівництва у м. Дніпро сучасного швидкісного виробничого комплексу загальною площею 12 000 м². На сьогоднішній день ТОВ «МІРОПЛАСТ» є лідером ринку ПВХ-профілю в Україні і одним з найбільших підприємств галузі в Східній Європі. Профільні системи ПВХ дозволяють створювати функціональні і естетичні вікна і двері для дому, офісу, комерційних і виробничих приміщень, забезпечуючи безпеку і відмінну звуко- і теплоізоляцію. Асортимент продукції компанії представлений брендами:

WDS, Galaxy, Olimpia забезпечує задоволення запитів найвимогливіших покупців, що працюють в різних сферах діяльності.

Місія компанії: бути світовим лідером у продажах, виробництві ПВХ-профілю з відмінною якістю.

Мета: Зайняти лідируючі позиції у виробництві металопластикових вікон як в Україні, так і в інших країнах.

В 2019 р. Компанія «МІРОПЛАСТ» була визнана лідером українського ринку за обсягами виробництва ПВХ-профілю згідно з дослідженням компанії Pro-Consulting. Показники ТОВ «МІРОПЛАСТ», виробника профільних систем під торговою маркою WDS, перевершили показники найближчого конкурента майже в два рази. Більш того, компанія зайняла найбільшу частку на ринку ПВХ-профілю в цілому серед інших виробників і імпортерів. В 2020 році компанія закріпила лідерство на ПВХ-ринку України, утримуючи позицію №1 в продажах 5 років поспіль (з часткою в продажах на українському ринку 42%). Друге та третє місце посідають компанії «Маядо» (22,2%) та «Опентек» (16,7%).

Всього в Україні в 2020 році було реалізовано близько 79 тисяч тонн ПВХ. Трійка лідерів виглядає наступним чином:

- ТОВ «Міропласт» (ТМ WDS) - 21 тис. тонн
- ТОВ «Маядо» (ТМ WINTECH) - 17,5 тис. тонн
- ТОВ «Опентек» (ТМ OPEN TESC) - 14 тис. тонн

Крім лідерства серед виробників, компанія МІРОПЛАСТ зайняла перше місце серед українських експортерів ПВХ-профілю. У 2020 компанія експортувала продукцію в 20 країн, серед яких країни СНД, Балканські країни, Італія, Німеччина, Південна Корея і Перу.

Потужності компанії дозволяють виробляти до 5870 тонн готової продукції в місяць.

Географія та структура продажів продукції компанії наведена на рис.2.1.

Слід зазначити, що основну частку продукції ТОВ «МІРОПЛАСТ» реалізує на внутрішньому ринку (62%). На експорт було відвантажено 38% від загальних продаж; продукція відвантажувалася у більш ніж 20 країн, найбільша доля відвантажень у країни СНД, а саме в Білорусь, Грузію, Казахстан.

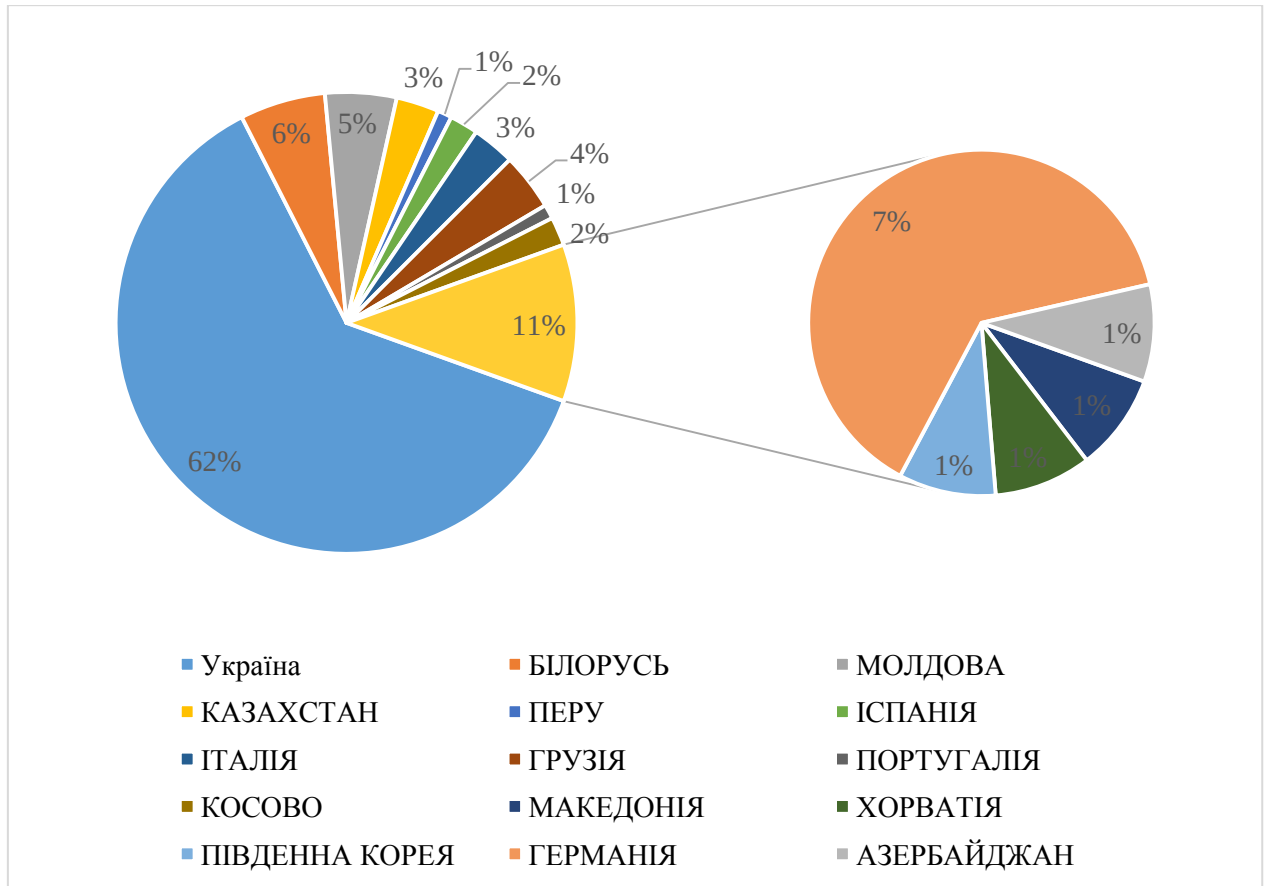


Рисунок 2.1 – Географія продажу продукції ТОВ «МІРОПЛАСТ»

Організаційна структура ТОВ «МІРОПЛАСТ» наведена на рисунку 2.2.

Організаційна структура компанії є лінійно-функціональною.

Основним принципом управління ТОВ «МІРОПЛАСТ» є розмежування повноважень і відповідальності за функціями та прийняття рішень по вертикалі. Управління здійснюється за лінійною схемою, а функціональні підрозділи допомагають лінійним керівникам у вирішенні відповідних управлінських функцій.

Генеральний директор компанії здійснює поточне керівництво всією діяльністю Товариства. Кожен співробітник компанії, який працює в тому чи іншому відділі Товариства має певні функції та обов'язки.

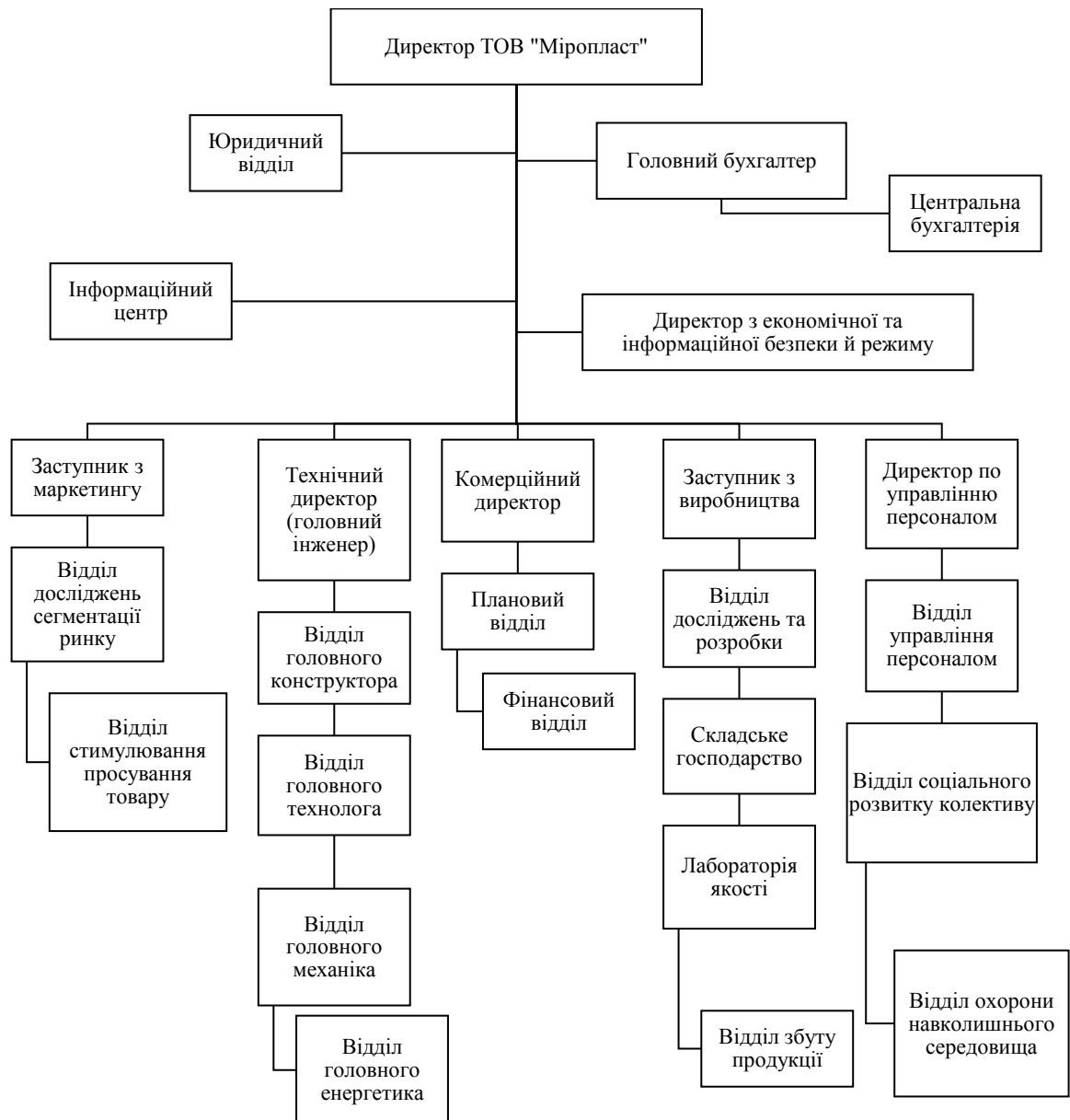


Рисунок 2.2 - Організаційна структура ТОВ «МІРОПЛАСТ»

Важливим вектором діяльності компанії є забезпечення високого рівня інформаційної безпеки. Даний напрямок в компанії здійснюється підрядною організацією ІП Дунаєнко за заключним довгостроковим договором підряду між керівництвом компанії в особі Директора з економічної та інформаційної безпеки й режиму та керівником підрядної компанії. Захист інформації на

підприємстві є дуже важливою річчю і цей аспект є обов'язковим при укладанні контракту компанією з її працівниками, особливо з керівниками. Забезпечення інформаційної безпеки на підприємстві полягає постійному контролі за джерелами виникнення потенційних загроз (антропогенні, технологічні та стихійні джерела) та необхідності здійснювати захист інформації різними способами (захист інформації від копіювання та ін.).

Аналіз основних техніко-економічних показників діяльності ТОВ «МІРОПЛАСТ» в 2019-2020рр. наведено в табл.2.1.

Таблиця 2.1 - Аналіз основних техніко-економічних показників діяльності ТОВ «МІРОПЛАСТ» в 2019-2020рр.

Показники	Роки		Відхилення 2020/2019	
	2019	2020	Абсолютне, (+/-)	Відносне, (%)
Виробнича потужність, тис. тонн	90	90	0	0,00
Випуск продукції в натуральному вираженні, тис.тонн	68,55	70,44	1,89	2,76
Реалізована продукція (обсяг реалізації), тис. грн..	950925,5	1078327	127401,4	13,40
Середньорічна вартість основних виробничих фондів, тис. грн..	184054,2	203864,1	19809,9	10,76
Чисельність працюючих, осіб	600	597	-3	-0,50
Фонд оплати праці, тис. грн..	61380,2	64117,8	2737,6	4,46
Середня з/п, грн..	8525,028	8950,0	424,9722	4,98
Повна собівартість товарної продукції, тис. грн..	716422,8	830385,7	113962,9	15,91
Чистий прибуток, тис. грн..	15504,3	22617,1	7112,8	45,88
Продуктивність праці, тис.грн.	1584,876	1806,243	221,3669	13,97
Витрати на 1 грн. товарної продукції, грн..	0,753395	0,770069	0,016673	2,21
Рентабельність продажу	1,116	1,554	0,438	39,25

В результаті аналізу техніко-економічних показників маємо зробити наступні висновки: на підприємстві спостерігається позитивна тенденція до збільшення обсягів випуску продукції. В 2020 р. було вироблене 70,44 тонн продукції, що більше на 1,89 тис.тонн ніж в 2019 р.. Обсяги реалізації також звеличились на 13,4% та склали на кінець 2020 р. – 1078327 тис.грн.

За даними таблиці 2.1 обсяг виробленої та реалізованої продукції протягом 2019-2020рр. має позитивну динаміку до зростання. Так, обсяг

виробленої продукції у 2020 році порівняно з 2019 роком збільшився на 1,89 тис. тонн (2,76%). Причиною темпу зростання є використання усіх виробничих потужностей підприємства. Обсяг реалізації у 2020 році порівняно з 2019 роком зріс на 127401,4 тис. грн., темп зростання обсягу реалізації становить 13,4%. Середньорічний темп приросту обсягів виробництва складає 2,76%, а реалізації – 13,4%. Це свідчить про зменшення залишків нереалізованої продукції на складах підприємства.

Основні засоби на в компанії враховуються за первісною (умовною) вартістю мінус подальша амортизація і знецінення. Первісна вартість включає витрати, безпосередньо пов'язані з придбанням активів. Вартість активів, створених власними силами, включає вартість матеріалів, прямі витрати на оплату праці і відповідну частину виробничих витрат. Терміни користування основними засобами (за основними групами) визначені на підприємстві у таких діапазонах: - будівлі - 20-80 років; - споруди - 15-40 років; - передавальні пристрої - 10-50 років; - виробниче устаткування - 5-40 років; - транспортні засоби - 5-35 років; - інші основні засоби - 4-20 років.

Середньорічна вартість основних виробничих фондів збільшилась на 10,76% та склала на кінець 2020р. - 203864,1тис.грн. Дане підвищення відбулося за рахунок збільшення вартості машин та обладнання.

Чисельність працюючих компанії складає 597 осіб. Витрати на оплату праці щорічно зростають. За 2019-2020 рр. вони збільшились на 4,46% та склали на кінець 2020 р. - 64117,8 тис.грн. Продуктивність праці зросла на 13,97% та склала на кінець 2020 р. - 1806,243 тис.грн.

Негативною тенденцією в діяльності компанії є зростання собівартості продукції на 15,91%. На підвищення собівартості продукції підприємства суттєво вплинуло збільшення витрат на модернізацію обладнання, витрати на збут та підвищення тарифів за енергоносії. За 2020 р. було проведено модернізацію лабораторії з контролю якості, виробничих цехів компанії. Лабораторії було дооснащене новим сучасним лабораторним обладнанням з метою приведення їх у відповідність до вимог FDA. В цехах було

модернізовано електромережі, системи вентиляції, закуплено нове обладнання та прилади.

Компанія активно проводить реконструкцію інженерно-технічної інфраструктури. Одним з таких об'єктів в 2020 році стала компресорна, для якої було виконано наступні роботи: придбано та проведено монтаж нового повітряного компресора та абсорбційного осушувача, проведено пуско-налагоджувальні роботи та введення в експлуатацію.

Зросли витрати на 1 грн. товарної продукції на 0,01 коп. (2,21%). Істотним фактором, що впливає на величину витрат на 1 грн. товарної продукції, є зростання рівня собівартості продукції.

Позитивну динаміку демонструє зростання чистого прибутку та доходу від реалізації компанії. Так, за 2019-2020рр. прибутковість ТОВ «МІРОПЛАСТ» зросла на 45,88% (рис.2.4).

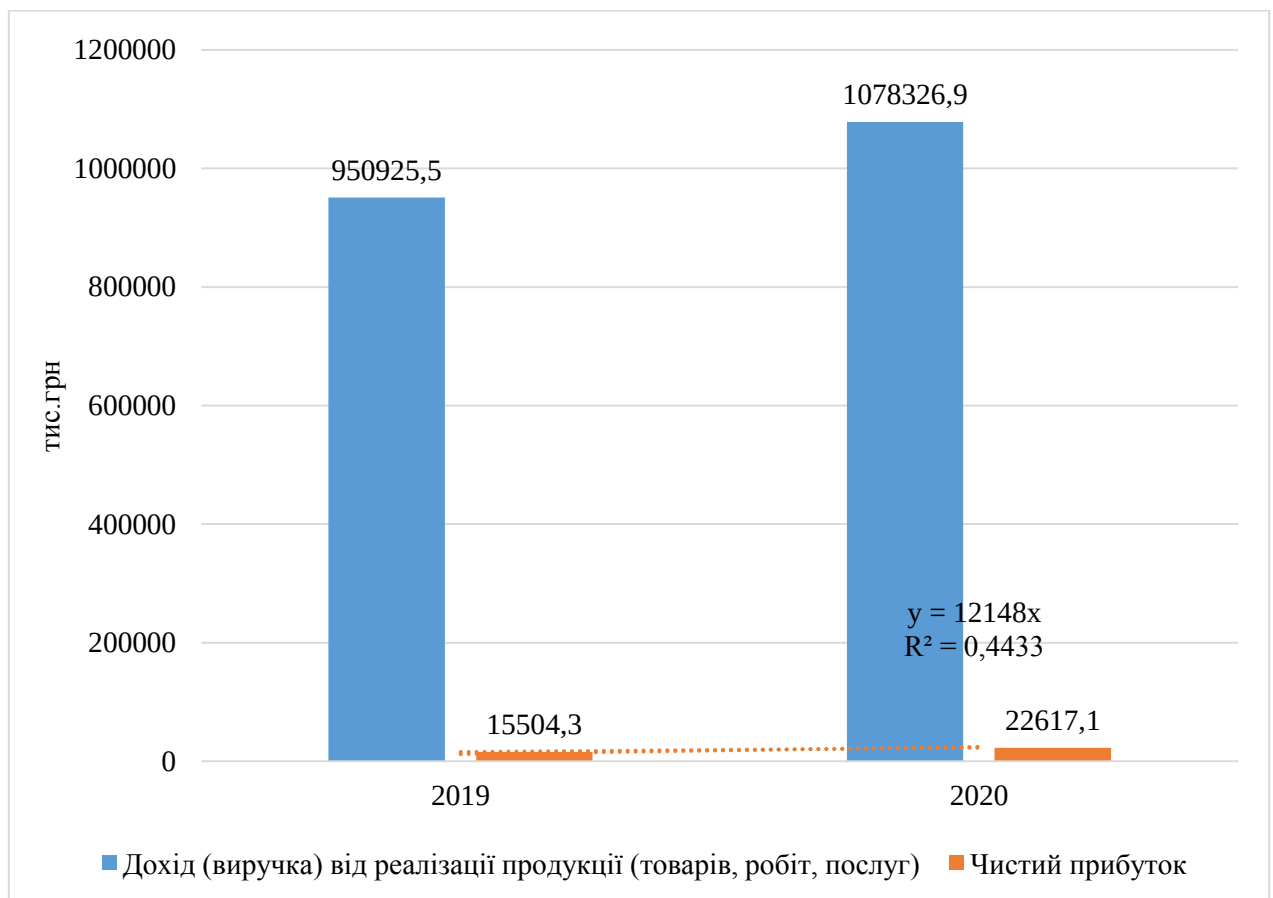


Рисунок 2.4 – Динаміка прибутковості компанії за 2019-2020 рр.

Основною причиною зростання чистого прибутку підприємства було значне зростання доходу від реалізації продукції наряду зі зростанням валового прибутку.

Отже, на ТОВ «МІРОПЛАСТ» спостерігається загальне покращення фінансово-господарської ситуації.

Нами були визначені основні фактори, що впливають на діяльність ТОВ «МІРОПЛАСТ» наведені в таблиці 2.2.

Таблиця 2.2 - Основні фактори, що впливають на діяльність ТОВ «МІРОПЛАСТ»

Група факторів	Опис проблем	Ступінь впливу на діяльність емітента			Які зміни, що прогнозуються, мають вплинути на підприємство
		незначний вплив	середній вплив	значний вплив	
Політичні	Недосконалість законодавства			+	Підвищення прибутковості та економічної активності підприємств вплине на підвищення платоспроможності
Фінансово-економічні	Неплатоспроможність підприємств			+	Неплатоспроможність підприємств
Виробничо-технологічні	Застаріле обладнання		+		Придбання нового обладнання
Соціальні	Погіршення фінансового стану підприємств			+	Результатом є зниження прибутку
Екологічні	Забруднення навколишнього середовища	+			Забруднення навколишнього середовища

Отже, на діяльність підприємства впливають значна кількість факторів з різним ступенем впливу Політичні, фінансово-економічні, соціальні фактори мають значний вплив на діяльність товариства.

Інформаційна підтримка діяльності підприємства залежить не тільки від наявності інформаційних ресурсів, а й від можливостей впровадження інформаційних інновацій, впорядкування інформаційних потоків підприємства, від вирішення проблем його ефективної інформаційної взаємодії з суб'єктами ринку.

Аналіз впливу факторів мікросередовища на діяльність ТОВ «МІРОПЛАСТ» приведений в табл.2.3.

Таблиця 2.3 - Аналіз впливу факторів мікросередовища на діяльність ТОВ «МІРОПЛАСТ»

Елементи мікросередовища	Фактори впливу на підприємство	Можливий прояв факторів на підприємстві в стратегічному періоді	(+) можливості
			(-) загрози
1. Конкурентне середовище, конкуренти	1.1. Можлива поява нових компаній в галузі	- посилення конкуренції	-
	1.2. Зниження цінового характеру конкуренції на вітчизняному та світовому ринках і т.д.	- втрата конкурентної переваги	-
2. Споживачі	2.1. Стабілізація економіки, підйом промисловості, підвищення рівня життя населення	- зростання попиту на продукцію компанії	+
	2.2. Зміна мотивації основних покупців з низької ціни на якість продукції	- додаткові витрати на підвищення якості продукції	-
3. Партнери	3.1. Поглиблення розподілу праці і розвитком кооперації	- забезпечення чималої долі постійного збуту продукції, можливість інвестування в оновлення виробництва	+
4. Постачальники	4.1. Підвищення тарифів постачальниками енергоресурсів	- зростання собівартості, зниження прибутковості	-
	4.2. Зниження ціни на основні комплектуючі матеріали виробництва	- зниження собівартості, зростання прибутковості	+
5. Інші елементи мікросередовища (місцеві органи партій, громадських організацій, влади)	5.1. Активізація профспілок із захисту інтересів робітників	- зростання витрат на соціальні потреби	+/-

В процесі діяльності ТОВ «МІРОПЛАСТ» потрібно пам'ятати, що недооцінка конкурентів і переоцінка ринків доводять навіть великі компанії до значних втрат і до криз. Треба розуміти, що споживачі - не єдиний об'єкт суперництва організацій. Останні можуть також вести конкурентну боротьбу за трудові ресурси, матеріали, капітал і право використовувати певні технічні

нововведення. Від реакції на конкуренцію залежать такі внутрішні чинники, як умови роботи, оплата праці і характер стосунків керівників з підлеглими. В той же час, потрібно відзначити, що конкуренція інколи штовхає фірми і на створення між ними угод різних типів від розділу ринку до кооперації між конкурентами. Крім конкурентів, покупців, партнерів, постачальників на діяльність компанії суттєво впливають інші елементи мікросередовища: місцеві органи влади, громадські організації, податкова адміністрація, пожежний нагляд, технагляд, Держстандарт та ін.

Далі проведемо аналіз зовнішнього та внутрішнього середовища організації (SWOT – аналіз) та наведемо його в таблиці 2.4.

Таблиця 2.4 - SWOT – аналіз ТОВ «МІРОПЛАСТ»

(strengths – сила, weaknesses – слабкості, opportunities – можливості, threats – небезпеки)

		Зовнішнє середовище	
		Можливості (шанси): - розширення виробництва; - входження у нові ринки; - поліпшення законодавства.	Загрози: - постійні зміни у законодавстві; - виникнення нових конкурентів
Внутрішнє середовище	Сильні сторони: - висока якість продукції; - кваліфікований персонал - наявність жорсткої виробничої дисципліни у колективі.	Заходи: - вихід на нові ринки збуту; - збільшення прибутків за рахунок збільшення обсягів продажу товарів	Заходи: - пошук стратегій протистояння можливим конкурентам
	Слабкі сторони: - висока конкуренція в галузі, достатньо висока ціна товарів даного сегменту ринку		

Після проведення SWOT – аналізу компанії, можна зробити висновок, що ТОВ «МІРОПЛАСТ» має достатньо сильних сторін, а також має чудові шанси для подальшого розвитку. При наявності високої конкуренції серед закордонних виробників ТОВ «МІРОПЛАСТ» міцно утримує свою нішу на ринку України та зарубіжних ринках. Що ж стосується слабких сторін, то підприємству варто направити свої зусилля на: освоєння нових ринків та

збільшенням обсягів продажу товарів; досягнення максимальних прибутків; постійно підвищувати рівень кваліфікації працівників; збільшити кількість каналів збуту та підтримувати конкурентоспроможність на даному сегменті ринку.

2.2 Аналіз фінансово-господарського стану ТОВ «МІРОПЛАСТ»

Проаналізуємо основні фінансово-господарські результати діяльності ТОВ «МІРОПЛАСТ» за допомогою наступних даних: Баланс (форма №1) на кінець 2019р., 2020 р.; Звіт про фінансові результати (форма №2) на кінець 2019р., 2020р. Основним звітним документом компанії є бухгалтерський баланс, який являє собою моментальний знімок фінансово-господарського стану підприємства на певну дату і дозволяє зробити оцінку найсуттєвіших ознак ТОВ «МІРОПЛАСТ». При проведенні аналізу фінансового стану ТОВ «МІРОПЛАСТ» використаємо порівняльний аналітичний аналіз балансу підприємства (табл. 2.5).

Таблиця 2.5 – Аналітичний баланс ТОВ «МІРОПЛАСТ» за 2019-2020рр.

Показник	Абсолютні величини (тис.грн.)		Питома вага, %		Зміни			
	2019р	2020р.	2019р	2020р.	в абсол. величинах (3 - 2) (тис.грн)	у питомій вазі (5 - 4) (%)	у % на початок періоду (6:2* 100)	у % до зміни підсумку балансу (6:66*100)
1	2	3	4	5	6	7	8	9
Активи								
Необоротні	160433,8	186129,8	45,60	46,20	25696	-45,13	16,02	50,36
Оборотні активи	189649,2	214641,7	53,90	53,28	24992,5	-53,37	13,18	48,98
запаси	71723,1	82857,4	20,38	20,57	11134,3	-20,18	15,52	21,82
дебіт. заборгов.	62845	53510,6	17,86	13,28	-9334,4	-17,73	-14,85	-18,29
грошові кошти	12944	15999,9	3,68	3,97	3055,9	-3,64	23,61	5,99
ін. оборотні активи	0	0	0,00	0,00	0	0,00	0,00	0,00
Інші активи	1775,2	2113,7	0,50	0,52	338,5	-0,50	19,07	0,66
Баланс	351858,2	402885,2	100,00	100,00	51027	-99,00	14,50	100,00
Пасиви								
Власний капітал	193706,6	209029	55,05	51,88	15322,4	-54,53	7,91	30,03
Довгострокові зобов'язання	26881	0	7,64	0,00	-26881	-7,64	-100,00	-52,68
Поточні	131270,6	193856,2	37,31	48,12	62585,6	-36,83	47,68	122,65

зобов'язання								
короткострокові кредити банків	31069,1	0	8,83	0,00	-31069,1	-8,83	-100,00	-60,89
кредиторська заборгованість	100201,5	193856,2	28,48	48,12	93654,7	-28,00	93,47	183,54
інші поточні зобов'язання	0	0	0,00	0,00	0	0,00		0,00
Інші пасиви	0	0	0,00	0,00	0	0,00		0,00
Баланс	351858,2	402885,2	100,00	100,00	51027	-99,00	14,50	100,00

На підставі даних табл. 2.5 можна зробити такі аналітичні висновки. За період 2019-2020рр. майно підприємства збільшилося на 51027 тис. грн. і становить на кінець періоду 402885,2 тис. грн. Така зміна обумовлена збільшенням необоротних активів на 25696 тис. грн. та за рахунок оборотних активів – на суму 24992,5 тис.грн.

Наведені дані дозволяють зробити такі висновки: Загальна сума активів збільшилась на 51027,0 тис. грн. або більш, ніж на 14,5%. Це збільшення відбулось переважно за рахунок значного зростання запасів (на 42 595,10 тис.грн.), необоротних активів (на 25696,0 тис.грн.) та оборотних активів (24 992,50 тис.грн.). У той же час, значно збільшилась сума основних засобів підприємства на 10,76% (в абсолютному вимірюванні – на 19809,9 тис. грн.). Це відбулось внаслідок купівлі обладнання для переоснащення виробництва.

Що стосується структури оборотних коштів, то можна зазначити, що вона поліпшилась та складає в структурі балансу 53,28%. Виробничі запаси збільшилися за період 2019-2020 рр. на 11134,3 тис. грн або на 15,52%. Величина дебіторської заборгованості складає 53510,6 тис. грн. За період 2019-2020рр. вона знизилась на 9334,4 тис. грн (14,85%).

Статутний капітал компанії складає 37008,2 тис.грн. При аналізі пасивів підприємства слід зазначити, що власний капітал зріс на 15 322,40 тис.грн. (7,91%) та складає на кінець 2020 р. 209029,0 тис.грн. Власний капітал підприємства знаходиться на рівні 55,05% - в 2019 році і 51,88 % - в 2020 році від загальної суми пасивів, що говорить про досить високу платоспроможність й не високий рівень ризику підприємства стати банкрутом.

Довгострокові зобов'язання знизились на 7,64%. На кінець 2020р. підприємство повністю розрахувалось із довгострокових зобов'язань.

Поточні зобов'язання підприємства значно зросли, за період 2019-2020рр. вони збільшилися на суму 62 585,60 тис. грн. (47,68%). Негативним явищем є наявність досить великої частки короткострокових заборгованостей, які у структурі пасивів займають за звітний період 2010-2020рр. - 37,31-48,12%. Негативною тенденцією в діяльності підприємства є значне зростання кредиторської заборгованості за товари, роботи, послуги (на 93 654,70 тис. грн., 93,47%). Це свідчить, що ТОВ «МІРОПЛАСТ» невчасно розрахувалося з постачальниками та підрядчиками за виконані роботи та отримані послуги.

Отже, основними висновками, зробленими при аналізі балансу підприємства можуть бути такі: структура статей балансу демонструє тенденцію до зростання частки основних засобів і незначного зменшення частки оборотних активів. Аналіз балансу ТОВ «МІРОПЛАСТ» за 2019-2020рр. свідчить, що підприємству слід покращити показники фінансової стійкості та ліквідності, а саме: поліпшити взаємовідносини із постачальниками і споживачами продукції, вдатися до поліпшення ситуації із дебіторською заборгованістю підприємству; поліпшити структуру оборотних коштів, більш продуктивно використовувати нове обладнання, збільшити обсяг продукції, що виготовляється; зменшити поточну заборгованість підприємства, намагатися перейти від короткострокових до довгострокових кредитів банку. Керівництву компанії слід вдатися до аналізу структури видатків, налагодити більш стабільні зв'язки з постачальниками, а також посилити контроль за витратами, запобігаючи нецільового витрачання ресурсів.

Аналіз ліквідності балансу полягає у порівнянні засобів по активу, згрупованих за ступенем їх ліквідності і розташованих у порядку зменшення ліквідності, із зобов'язаннями по пасиву, згрупованих за термінами їх погашення і розташованих у порядку зростання термінів (табл. 2.6).

Для визначення ліквідності балансу слід порівняти підсумки наведених груп по активу і пасиву. Баланс вважається абсолютно ліквідним, коли мають місце наступні співвідношення: $A1 \geq P1$; $A2 \geq P2$; $A3 \geq P3$; $A4 < P4$.

Результати розрахунку свідчать про недостатню ліквідність балансу ТОВ «МІРОПЛАСТ» протягом періоду 2019-2020 рр.

Таблиця 2.6 - Баланс ліквідності ТОВ «МІРОПЛАСТ» за 2019-2020рр.
(тис.грн)

Код	Назва	Опис	2019р	2020р
A1	Найбільш ліквідні активи	Грошові кошти	12944	15999,9
P1	Найбільш термінові зобов'язання	Кредиторська заборгованість	100201,5	193856,2
A1-P1	Забезпечення зобов'язань P1	Плюс добре, мінус погано	-87257,5	-177856
A2	Активи, які швидко реалізуються	Дебіторська заборгованість	62845	53510,6
P2	Короткострокові пасиви	Короткострокові позики	31069,1	0
A2-P2	Забезпечення зобов'язань P2	Плюс добре, мінус погано	31775,9	53510,6
A3	Активи, які повільно реалізуються	Запаси	71723,1	82857,4
P3	Довгострокові пасиви	Довгострокові позики	26881	0
A3-P3	Забезпечення зобов'язань P3	Плюс добре, мінус погано	44842,1	82857,4
A4	Активи, які важко реалізуються	Основні засоби	141863,5	170098,5
P4	Постійні пасиви	Власний капітал	193706,6	209029
A4-P4	Забезпечення зобов'язань P4	Плюс погано, мінус добре	-51843,1	-38930,5

Протягом 2019-2020 рр. нерівність $A1 > P1$ не виконується: це свідчить про недостатню платоспроможність підприємства на момент складання балансу і свідчить, що в компанії недостатньо коштів для покриття найбільш термінових зобов'язань абсолютно і найбільш ліквідних активів.

Так як в аналізованому періоді 2019-2020 рр. виконується нерівність $A2 > P2$, то швидко реалізовані активи перевищують короткострокові пасиви та організація може бути платоспроможною в недалекому майбутньому з урахуванням своєчасних розрахунків з кредиторами, отримання коштів від продажу продукції в кредит.

Також протягом періоду 2019-2020 рр. виконується нерівність $A3 > ПЗ$, то в майбутньому при своєчасному надходженні грошових коштів від продажу та платежів підприємство може бути платоспроможним на період, рівний середньої тривалості одного обороту оборотних коштів після дати складання балансу.

Далі проаналізуємо звіт про фінансові результати (табл. 2.7).

Таблиця 2.7 – Аналіз фінансових результатів ТОВ «МІРОПЛАСТ» за 2019-2020 рр.

Назва статті	Абсолютні величини (тис.грн)		Питома вага, %		Зміни, 2020/2019			
	2019р	2020р.	2019р	2020р	(+/-) (3 - 2) (тис.грн.)	(%) (5 - 4)	у % до поперед. періоду (6 : 2 * 100)	у % до зміни загальн.велич. (6 : 6р * 100)
1	2	3	4	5	6	7	8	9
Доходи								
Виручка	950 925,5	1 078 326,9	92,43	92,98	+127 401,4	+0,55	+13,40	+97,31
Інші операційні доходи	53 961,9	53 673,2	5,25	4,63	-288,70	-0,62	-0,54	-0,22
Фінансові доходи	17 338,60	20 329,3	1,69	1,75	+2 990,70	+0,07	+17,25	+2,28
Інші доходи	6 570,80	7 393,30	0,64	0,64	+822,50	0,00	+12,52	+0,63
Разом	1 028 796,8	1 159 722,7	100,00	100,00	+130 925,9	0,00	+12,73	+100,00
Витрати								
Непрямі податки	135 617,5	147 863,20	13,38	13,00	+12 245,70	-0,38	+9,03	+9,89
Собівартість продукції	716 422,8	830 385,70	70,70	73,03	+113 962,9	+2,32	+15,91	+92,04
Операційні витрати	143 747,3	139 289,80	14,19	12,25	-4 457,50	-1,94	-3,10	-3,60
Фінансові витрати	6 476,90	7 328,50	0,64	0,64	+851,60	+0,01	+13,15	+0,69
Інші витрати	6 844,70	5 842,30	0,68	0,51	-1 002,40	-0,16	-14,64	-0,81
Податок на прибуток	4 183,30	6 396,10	0,41	0,56	+2 212,80	+0,15	+52,90	+1,79
Разом	1 013 292,5	1 137 105,6	100,00	100,00	+123 813,1	0,00	+12,22	+100,00
Елементи операційних витрат								
Матеріальні затрати	399 073,80	432 389,50	88,75	87,19	+33 315,70	-1,57	+8,35	+71,97
Витрати на оплату праці	61380,2	64117,8	3,04	4,19	+2737,6	+4,46	+51,94	+15,36
Відрахування на соціальні заходи	9 876,20	11 038,30	2,20	2,23	+1 162,10	+0,03	+11,77	+2,51

Амортизація	11 976,40	18 046,50	2,66	3,64	+6 070,10	+0,98	+50,68	+13,11
Інші операційні витрати	15 035,00	13 670,00	3,34	2,76	-1 365,00	-0,59	-9,08	-2,95
Разом	449 649,40	495 942,20	100,00	100,00	+46 292,80	0,00	+10,30	+100,00

Цей аналіз дає змогу проаналізувати, які фактори вплинули в звітному періоді на валовий прибуток підприємства та фінансовий результат від операційної діяльності підприємства та на фінансовий результат від звичайної діяльності до оподаткування. Отже, в 2019-2020 рр. спостерігається збільшення суми чистого доходу (виручки) від реалізації продукції на 127401,4 тис.грн. Фінансові доходи в компанії зросли на 17,25% та склали на кінець 2020р. 20329,3 тис.грн. Інші операційні доходи на підприємстві за період 2019-2020рр. незначно знизились на 288,70 тис.грн. та склали на кінець 2020р. - 53 673,2 тис.грн.

Негативним моментом в діяльності компанії є збільшення собівартості продукції на 15,91% . В структурі витрат питома вага собівартості складає 73,03%. В результаті дослідження структури витрат ТОВ «Міропласт» в 2019-2020 рр. маємо зробити наступні висновки: операційні витрати в компанії мають тенденцію до зниження на 3,1%, фінансові витрати зросли на 13,1%.

Отже, в компанії за період 2019-2020 рр. спостерігається зростання витрат по багатьом позиціям, що негативно відображується на діяльності підприємства. Загалом, сума витрат збільшилась на 12,22%.

Одним з найважливіших показників роботи підприємства є прибуток. Прибуток ТОВ «МІРОПЛАСТ» за 2019-2020 рр. має склад, показаний в таблиці 2.8.

Таблиця 2.8 - Аналіз прибутку ТОВ «МІРОПЛАСТ» за 2019-2020 рр., тис.грн.

Показник	2 019р.	2 020р.	Абсолютне відхилення 2020/2019 (+/-)
1	2	3	4
Прибуток від реалізації продукції (валовий дохід)	98885,2	100078,0	1192,8
Прибуток від операційної діяльності	9099,8	14461,4	5361,6

Прибуток від звичайної діяльності	19 687,6	29013,2	9325,6
Податок на прибуток від звичайної діяльності	4183,3	6396,1	2212,8
Чистий прибуток (збиток)	15504,3	22617,1	7112,8

Балансовий прибуток ТОВ «МІРОПЛАСТ» включає в себе результати від реалізації продукції, робіт та послуг, від іншої реалізації, доходи та витрати від позареалізаційних операцій. Найважливішим джерелом формування прибутку є валовий дохід від продажів. У промисловості він дорівнює виторгу за мінусом матеріальних витрат на виробництво.

Показники прибутку підприємства мають позитивну тенденцію до зростання. Так, за період 2019-2020 рр. валовий дохід підприємства збільшився на суму 1192,8 тис.грн. та склав 100078,0 тис.грн. Чистий прибуток збільшився на 7112,8 тис.грн. та склав 22617,1 тис.грн.

Аналізуючи рівень прибутку, необхідно особливу увагу приділяти його динаміці. У зв'язку з тим, що динаміка характеризує розвиток явища в часі, аналіз динаміки уможлиблює прогнозування майбутнього рівня прибутку і на цій основі – визначення перспективних напрямків розвитку підприємства.

На рисунку 2.5 зображена динаміка прибутку ТОВ «МІРОПЛАСТ» за 2019-2020 рр.. Прибуток або збиток підприємства є головним показником, що відображає фінансовий результат, що складає із сукупності доходів і видатків, що виникають у результаті здійснення господарських операцій.

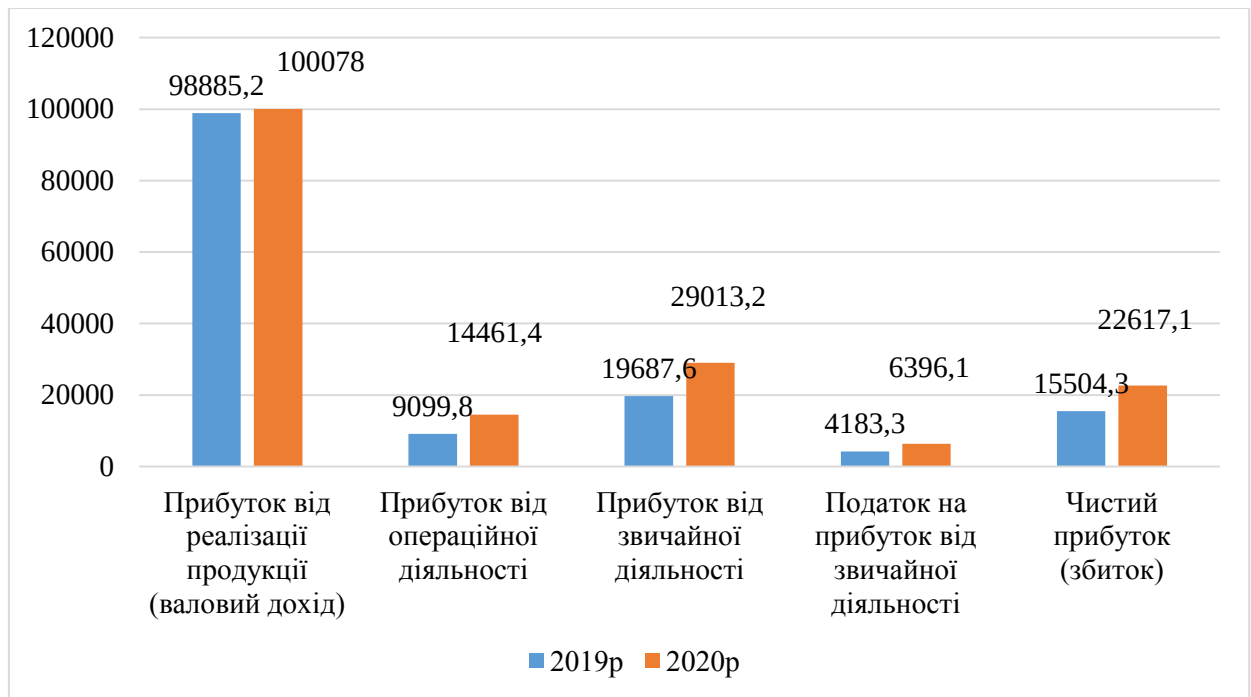


Рисунок 2.5 - Динаміка прибутку ТОВ «МІРОПЛАСТ» за період 2019-2020 рр..

В даному випадку в 2019-2020 рр. спостерігається покращення усіх показників прибутковості підприємства.

Аналіз основних показників рентабельності ТОВ «МІРОПЛАСТ» за 2019-2020рр.. наведемо в таблиці 2.9.

Таблиця 2.9 - Аналіз показників рентабельності ТОВ «МІРОПЛАСТ» за 2019-2020 рр.

Показники прибутковості	Розрахункова формула	Роки		Зміни, 2020/2019	
		2019р	2020р	(+/-)	(%)
Рентабельність активів	Чистий прибуток / Середньорічна вартість активів	4,643	5,993	1,35	29,08
Рентабельність власного капіталу	Чистий прибуток / Середньорічна вартість власного капіталу	8,338	11,232	2,894	34,71
Рентабельність продажу	Операційний прибуток / Чиста виручка	1,116	1,554	0,438	39,25
Рентабельність чистих активів	Чистий прибуток / Середньорічна вартість чистих активів	7,254	10,529	3,275	45,15
Рентабельність оборотних активів	Операційний прибуток / Середньорічна вартість оборотних активів	5,300	7,154	1,854	34,98

За проведеними розрахунками на підприємстві спостерігається зростання усіх показників рентабельності, що свідчить про покращення використання залучених ресурсів.

Рентабельність продажів - є одним з найважливіших показників ефективності діяльності компанії. Цей коефіцієнт показує, яку суму операційного прибутку одержує підприємство з кожної гривні проданої продукції. Іншими словами, скільки залишається в підприємства коштів після покриття собівартості продукції. Нормальною вважається рентабельність не менша 30%, в умовах високого податкового тиску – 15%.

За період 2019-2020 рр. в компанії спостерігається зростання даного показника на 39,25% та складає на кінець 2020 р. – 1,55, що є позитивним в діяльності компанії. Рентабельність активів також має тенденцію до зростання на 29,08% та складає на кінець 2020 р. - 5,99.

Зростання всіх коефіцієнтів рентабельності протягом аналізованого періоду 2019-2020 рр. свідчить про покращення результатів діяльності підприємства.

Фінансовий стан підприємства в короткостроковій перспективі оцінюється показниками ліквідності, ділової активності та фінансової стійкості.

Аналіз даних показників проведемо за допомогою засобів Excel та приведемо в таблицях 2.10 -2.11.

Таблиця 2.10 - Аналіз показників ліквідності та ділової активності ТОВ «МІРОПЛАСТ» за 2019-2020 рр.

Назва	Формула	Роки		Зміни, 2020/2019	
		2019р	2020р	(+/-)	(%)
Показники ліквідності					
Коефіцієнт абсолютної ліквідності	Грошові кошти / Поточні зобов'язання	0,305	0,149	-0,156	-51,15
Коефіцієнт проміжної ліквідності	(Оборотні активи - товарно-матеріальні запаси) / Поточні зобов'язання	0,898	0,518	-0,38	-42,32
Коефіцієнт загальної ліквідності (покриття)	Оборотні активи / Поточні зобов'язання	1,445	1,107	-0,338	-23,39
Власний оборотний капітал	Власний капітал - Необоротні активи	58378,6	20785,5	-37593,1	-64,40

Показники ділової активності					
Оборотність дебіторської заборгованості	Виручка від реалізації / Середньорічна вартість дебіторської заборгованості	46,426	40,422	-6,004	-12,93
Оборотність кредиторської заборгованості	Собівартість реалізованої продукції / Середньорічна вартість кредиторської заборгованості	8,655	6,987	-1,668	-19,27
Період погашення дебіторської заборгованості, днів	Кількість днів у періоді / Оборотно-кредиторська заборгованість	7,862	9,030	1,168	14,86
Період погашення кредиторської заборгованості, днів	Кількість днів у періоді / Оборотно-дебіторська заборгованість	42,173	52,239	10,066	23,87
Оборотність постійних активів	Виручка від реалізації / Середньорічна вартість постійних активів	5,079	5,370	0,291	5,73
Оборотність активів	Виручка від реалізації / Середньорічна вартість активів	2,441	2,466	0,025	1,02
Оборотність чистих активів	Виручка від реалізації / Середньорічна вартість чистих активів	3,626	3,781	0,155	4,27
Оборотність товарно-матеріальних запасів	Собівартість реалізованої продукції / Середньорічна вартість товарно-матеріальних запасів	10,824	8,927	-1,897	-17,53
Період обороту товарно-матеріальних запасів, днів	Кількість днів у періоді / Оборотно-матеріальних запасів	33,722	40,888	7,166	21,25
Тривалість операційного циклу, днів	Період погашення дебіторської заборгованості + Період обороту товарно-матеріальних запасів	41,584	49,918	8,334	20,04

Показники ліквідності показують здатність підприємства ТОВ «МІРОПЛАСТ» розраховуватись за своїми зобов'язаннями за рахунок наявних активів. Із таблиці 2.11 можна зробити висновок, що ліквідність підприємства за період 2019-2020 рр. має негативну тенденцію до зниження. Так, наприкінці 2020 року проти 2019 року становище з абсолютною ліквідністю погіршилось з 0,305 – 2019 р. до 0,149 – в 2020 р. та є нижчим за норму (0,2-0,35). Коефіцієнт абсолютної ліквідності показує, яка частина поточних (короткострокових) зобов'язань може бути погашена негайно.

Нормативне значення коефіцієнта покриття повинне бути не менше 2,0-2,5. Коефіцієнт покриття на кінець 2020 р. дорівнює 1,107 та свідчить про неможливість підприємства погасити поточні зобов'язання.

Коефіцієнт покриття, розрахований за даними підприємства, діяльність якого аналізується, знизився на 0,338 за рахунок зниження дебіторської заборгованості та матеріальних запасів у межах необхідної потреби та складає на кінець 2020 року 1,107. Це означає, що на кожну 1 гривню поточних зобов'язань (боргів) підприємство має 1,107 грн. поточних активів. Негативною тенденцією можливо визнати зниження величини власного капіталу підприємства на суму - 37593,1 тис. грн. (64,4%).

Динаміка показників ліквідності говорить про ріст ризикованості діяльності ТОВ «МІРОПЛАСТ» за 2019-2020 рр. з погляду неповернення боргів і зниження реального рівня платоспроможності.

Аналіз ділової активності дозволяє проаналізувати ефективність основної діяльності ТОВ «МІРОПЛАСТ» за 2019-2020 рр., що характеризується швидкістю обертання фінансових ресурсів підприємства. Аналіз здійснюється за допомогою коефіцієнтів оборотності.

Ефективність управління ТОВ «МІРОПЛАСТ» визначається темпами прискорення обертання ресурсів, що повинно знаходити своє відображення у зростанні відповідних показників. Нормативного значення показників не має, але чим швидше обертаються ресурси підприємства, тим краще. Підвищення обертання ресурсів є, поряд з високою прибутковістю другим важелем підвищення фінансового благополуччя підприємства.

Низький рівень коефіцієнтів обертання активів може свідчити про недостатню завантаженість та низьку ефективність експлуатації виробничих потужностей, зростання дебіторської заборгованості та запасів.

Показники ділової активності показують швидкість використання залучених ресурсів.

Показник оборотності активів показує, скільки разів за період обертається капітал, вкладений в активи підприємства: в 2019 р. даний показник склав 2,44.; в 2020 р. – 2,46. Збільшення даного показника за період 2019-2020 рр. на 1,02% говорить про покращення ефективності їхнього

використання. За аналізований період 2019-2020 рр. оборотність чистих активів зросла на 4,27% та склала 3,78.

Період обороту товарно-матеріальних запасів зріс на 7 днів та склав на кінець 2020 р. - 40,88 днів. Тривалість операційного циклу зросла на 8,33 дня та склала на кінець 2020р. – 49,9 днів.

В результаті проведеного аналізу показників ділової активності ТОВ «МІРОПЛАСТ» за 2019-2020 рр. маємо зробити наступні висновки: підвищення ефективності діяльності підприємства можливо здійснити за рахунок прискорення обертання ресурсів і скорочення періоду їх обігу. Збільшення числа обертів можливе шляхом скорочення періоду виробництва або скорочення періоду обігу.

Скорочення періоду виробництва потребує вдосконалення технології, модернізації і автоматизації виробництва.

Скорочення періоду обігу потребує більш ефективного і раціонального використання ресурсів, прискорення документообігу і розрахунків.

Показники фінансової стійкості показують залежність підприємства від зовнішніх джерел фінансування. За період 2019-2020 рр. фінансова стійкість ТОВ «МІРОПЛАСТ» знизилась (табл.2.11).

Таблиця 2.11 - Аналіз показників фінансової стійкості ТОВ «МІРОПЛАСТ» за 2019-2020 рр.

Назва	Формула	Роки		Зміни, 2020/2019	
		2019р	2020р	(+/-)	(%)
Коефіцієнт фінансової незалежності (автономії)	Власний капітал / Активи	0,551	0,519	-0,032	-5,81
Коефіцієнт фінансової залежності	Активи / Власний капітал	1,816	1,927	0,111	6,11
Коефіцієнт заборгованості	Позикові кошти / Активи	0,449	0,481	0,032	7,13
Відношення довгострокових кредитів до капіталізації	Довгострокові кредити / Капіталізація	0,122	0,000	-0,122	-100,00
Відношення довгострокових кредитів до власного капіталу	Довгострокові кредити / Власний капітал	0,139	0,000	-0,139	-100,00
Відношення заборгованості до власного капіталу	Позичені кошти / Власний капітал	0,816	0,927	0,111	13,60

Фінансова стійкість – характеристика стабільності фінансового стану підприємства, яка забезпечується високою часткою власного капіталу в загальній сумі використовуваних фінансових засобів. Саме фінансова стійкість ТОВ «МІРОПЛАСТ» характеризує ефективність операційного, інвестиційного і фінансового розвитку, містить необхідну інформацію для інвесторів, постачальників та власників. Фінансова стійкість підприємства тісно пов'язана із перспективною його платоспроможністю. Тому одним з найважливіших завдань, що постає перед ТОВ «МІРОПЛАСТ» є підвищення рівня фінансової стійкості. За результатами розрахунків фінансової стійкості можна зробити висновки про підвищення рівня фінансової залежності.

Співвідношення позикових і власних коштів характеризує незалежність підприємства від зовнішніх позик. Значення даного коефіцієнта – 0,816 за 2019 р. та 0,927 за 2020 р. Низький рівень цього коефіцієнта (менш 1) відображає нестабільну ситуацію щодо грошових коштів підприємства. Висока залежність від зовнішніх позик погіршує стан підприємства у разі сповільнення темпів реалізації, оскільки витрати з виплати відсотків на позиковий капітал є умовно постійними. Однак, позитивна динаміка даного показника протягом 2019-2020 рр. свідчить про покращення ситуації щодо грошових коштів підприємства. Зниження залежності від зовнішніх позик істотно поліпшує стан підприємства у разі сповільнення темпів реалізації, оскільки витрати з виплати відсотків на позиковий капітал є умовно постійними.

Коефіцієнт фінансової незалежності (автономії) показує питому вагу власного капіталу в загальній сумі засобів, авансованих у його діяльність. Частина власного капіталу в загальній сумі фінансових ресурсів повинна бути не меншою 50%, тобто коефіцієнт незалежності $\geq 0,5$. Коефіцієнт фінансової незалежності (автономії) показує, що власних коштів в структурі капіталу ТОВ «МІРОПЛАСТ» на кінець 2020 р. становить 51,9 % та свідчить про те, що компанія характеризується значним запасом міцності ($0,519 > 0,5$).

Проте зниження за період 2019-2020 рр. свідчить про деяке погіршення фінансової незалежності компанії, а саме незначне погіршення фінансової структури коштів. Вона виражається в підвищенні питомої ваги позикового капіталу і зниженню рівня коштів, забезпечених власним капіталом.

Коефіцієнт фінансового левериджу розраховується як співвідношення довгострокового позикового капіталу і власного капіталу. Показник фінансового левериджу характеризує залежність підприємства від довгострокових зобов'язань. Збільшення даного показника за період 2019-2020рр. на -0,139 характеризує зниження залежності компанії від довгострокових зобов'язань. Узагальнюючи показники фінансової стійкості ТОВ «МІРОПЛАСТ», можна зробити висновок про наявність в компанії значного запасу фінансової міцності ($> 0,5$). Однак, фінансова стійкість підприємства поступово знижується, що є негативним моментом в діяльності підприємства. В умовах економічної кризи підтримання фінансової стійкості на достатньо високому рівні потребує впровадження систематичного управління комплексом заходів щодо запобігання зниження рівня цієї характеристики підприємства. Фінансово стійким можна вважати таке підприємство, яке за рахунок власних коштів спроможне забезпечити запаси й витрати, не допустити невиправданої кредиторської заборгованості.

2.3 Організація системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ»

Система управління інформаційною безпекою (СУІБ) ТОВ «МІРОПЛАСТ» являє собою частину загальної системи менеджменту компанії, засновану на ризик-орієнтованому підході, призначену для створення, реалізації, експлуатації, моніторингу, аналізу, підтримки та вдосконалення інформаційної безпеки (ІБ) компанії (рис. 2.6).



Рисунок 2.6 – Структура управління інформаційною безпекою ТОВ «МІРОПЛАСТ»

Одним з важливих етапів побудови системи інформаційної безпеки компанії є створення ефективного механізму управління доступом до інформації, тобто вирішення питань як розмежування доступу, так і визначення методів доступу. Інформація та матеріальні ресурси, які необхідно захищати, називаються об'єктами захисту. До них відноситься мовна інформація, інформація, що зберігається і обробляється за допомогою засобів зв'язку і інформатизації у вигляді різних носіїв інформації, документи на паперових носіях і ін.

Основними цілями побудови СУІБ є:

- забезпечення конфіденційності, цілісності та доступності інформаційних активів ТОВ «МІРОПЛАСТ»;
- виконання вимог безпеки клієнтів і партнерів;
- відповідність вимогам регуляторів, законодавства і галузевих нормативних документів.

Місце СУІБ в загальній системі менеджменту компанії наведено на рис. 2.7.

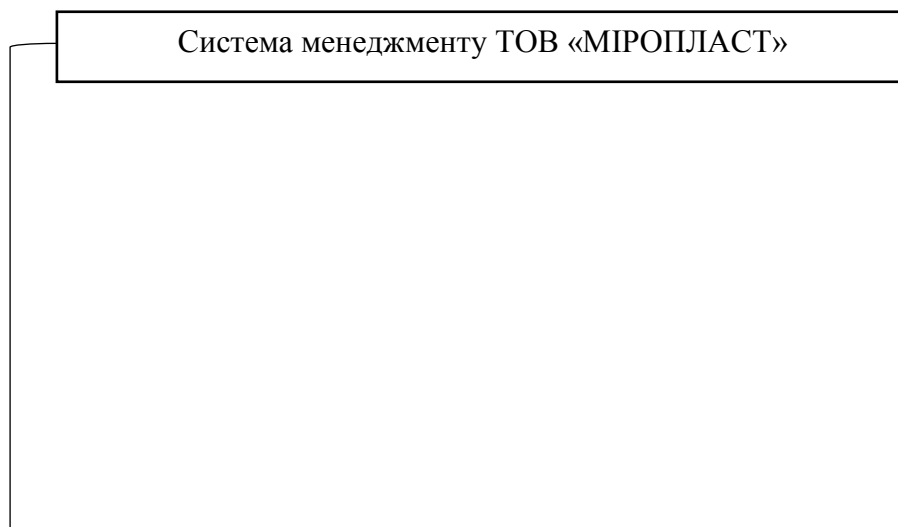




Рисунок 2.7 - Місце СУІБ в загальній системі менеджменту ТОВ «МІРОПЛАСТ»

Побудова СУІБ в компанії ТОВ «МІРОПЛАСТ» дозволяє чітко визначити, як взаємопов'язані процеси і підсистеми інформаційної безпеки (ІБ), хто за них відповідає, які фінансові та трудові ресурси необхідні для їх ефективного функціонування і ін. СУІБ включає (рис.2.8):

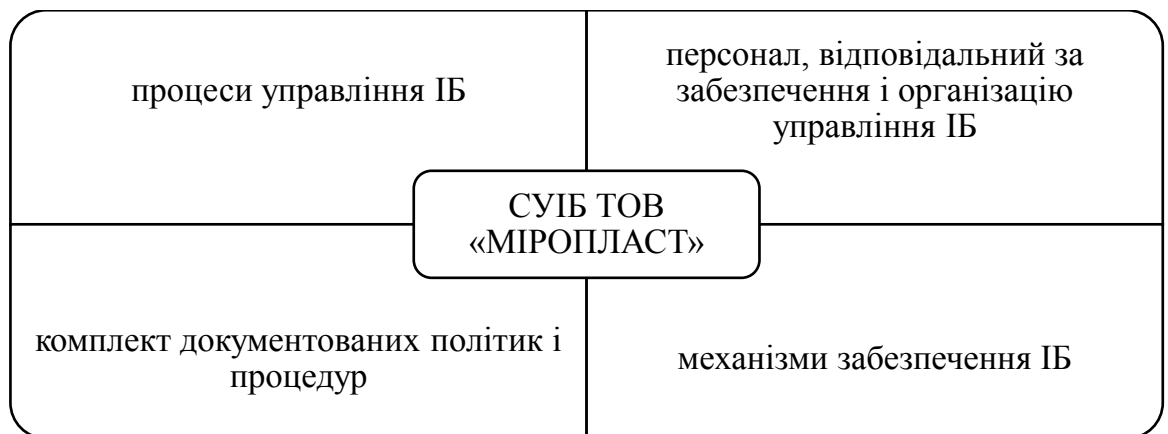


Рисунок 2.8 - Система управління інформаційною безпекою (СУІБ) ТОВ «МІРОПЛАСТ»

Політика інформаційної безпеки ТОВ «МІРОПЛАСТ» є внутрішнім нормативним документом компанії, що формулює та висловлює її позицію щодо інформаційної безпеки (ІБ), а також визначає основні принципи та завдання системи управління інформаційною безпекою (СУІБ) підприємства.

Політика є нормативною основою для захисту інформаційних активів компанії з метою забезпечення: конфіденційності – забезпечення доступності інформації тільки для авторизованих осіб, користувачів, процесів в мінімально необхідному обсязі; цілісності – захисту точності, коректності та повноти методів обробки інформації; доступності – забезпечення безперервного доступу до інформаційних і супутніх активів і сервісів компанії, згідно з наданими користувачам повноваженням і правами у мінімально необхідному обсязі; спостережності – забезпечення можливості визначення користувачів, процесів, що працюють з тим чи іншим інформаційним активом компанії, час та дату такої роботи, а також забезпечення принципу неможливості відмови від виконаних дій.

Інформаційна політика ТОВ «МІРОПЛАСТ» базується на вимогах законодавчих, регуляторних та нормативних документів з інформаційної безпеки. Дія Політики поширюється на всю компанію та всі треті сторони, які мають доступ до її інформаційних активів. Політика розроблена у відповідності до вимог чинного законодавства України, а саме: Законів України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних»; стандартів ДСТУ ISO/IEC 2700x:2015; інших нормативних документів, що регламентують вимоги до інформаційної безпеки.

Основними цілями управління інформаційною безпекою ТОВ «МІРОПЛАСТ» є: забезпечення безпеки персоналу та клієнтів компанії; управління інформаційною безпекою, у тому числі визначення ролей та обов'язків у галузі ІБ, створення і підтримка системи управління ІБ (СУІБ); класифікація інформаційних активів; здійснення оцінки ризиків інформаційної безпеки; забезпечення безпеки інформаційних активів відповідно до категорії їх класифікації та оцінки ризиків; моніторинг подій інформаційної безпеки (ШБ) та управління інцидентами ІБ; забезпечення безперервності бізнес-діяльності компанії; безпечне управління життєвим циклом інформаційної системи.

ТОВ «МІРОПЛАСТ» дотримується наступних правил в частині забезпечення інформаційної безпеки та безперебійної діяльності компанії: публічні сервіси та внутрішні мережі компанії відповідають вимогам стандартів з інформаційної безпеки; для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво компанії створює працівникам умови для систематичного навчання нормам та заходам інформаційної безпеки; в ТОВ «МІРОПЛАСТ» складаються, діють, систематично тестуються та оновлюються плани безперебійного функціонування діяльності компанії на випадок непередбачуваних (критичних) ситуацій.

Працівники ТОВ «МІРОПЛАСТ» беруть участь у підтримці відповідного рівня інформаційної безпеки в межах своїх обов'язків та повноважень і несуть відповідальність за його порушення в межах, встановлених чинним законодавством України та внутрішніми нормативними документами компанії.

ТОВ «МІРОПЛАСТ» використовує наступні вимоги щодо забезпечення інформаційної безпеки: створено та затверджено перелік відомостей, що містять інформацію (в тому числі, з обмеженим доступом); визначено перелік критичних процесів; встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів; забезпечується контроль фізичного та логічного доступу до всіх наявних ресурсів; забезпечується парольний захист програмних та сервісних ресурсів; забезпечується антивірусний захист програмних та сервісних ресурсів; забезпечується захист мережі; забезпечується захист віддаленого доступу до ресурсів мережі (локальної, мережі Інтернет, мереж інших організацій); забезпечується ідентифікація та автентифікація всіх визначених ресурсів; забезпечується криптографічний захист інформації.

Ефективна інформаційна безпека ТОВ «МІРОПЛАСТ» забезпечується шляхом безперервної участі працівників всіх підрозділів на всіх рівнях діяльності. Кожен підрозділ несе відповідальність за виконання нормативних

документів компанії з ІБ як частини своїх службових завдань. Керівництво активно підтримує безпеку в межах компанії шляхом чіткого регулювання, підтверджених зобов'язань, чітких призначень та визнання відповідальності за ІБ.

На ТОВ «МІРОПЛАСТ» створений та постійно працює Керівний орган з питань інформаційної безпеки, рішення якого є обов'язковими для виконання усіма працівниками компанії. Головою Керівного органу наказом призначено Директора з інформаційної безпеки, який відповідає за питання інформаційної безпеки компанії. До складу Керівного органу включено спеціаліста з питань інформаційної безпеки.

Увесь найманий персонал ТОВ «МІРОПЛАСТ», підрядники та користувачі третьої сторони (за необхідності) проходять належне навчання для поінформованості та регулярно отримують оновлені дані щодо політик і процедур компанії, суттєвих для їх посадових функцій (виконання покладених на них зобов'язань відповідно до укладених договорів). Найманий персонал, підрядники та користувачі третьої сторони погоджують і підписують документи щодо термінів та умов з найму, які встановлюють взаємні відповідальності щодо інформаційної безпеки.

ТОВ «МІРОПЛАСТ» описує та захищає наступні види ресурсів: інформаційні ресурси - інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у тому числі знання працівників, партнерів компанії, бази даних та вміст файлових ресурсів, документація, навчальні матеріали, описи процедур, архіви тощо; програмне забезпечення - прикладне програмне забезпечення та системне програмне забезпечення, незалежно від форми отримання (придбання, власної розробки, таке, що вільно розповсюджується), яке використовується працівниками та системами ТОВ «МІРОПЛАСТ» для роботи та взаємодії з клієнтами та іншими системами тощо; фізичні ресурси - працівники, апаратні засоби інфраструктури (сервери, робочі станції, міжмережеві екрани, багатофункціональні пристрої, телекомунікаційне

обладнання, мережеве обладнання тощо), носії даних (диски, накопичувачі тощо), меблі, приміщення, виробниче обладнання, інші технічні засоби тощо; сервісні ресурси - обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку тощо), інші технічні сервіси (опалення, освітлення, енергозабезпечення, кондиціювання повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням ресурсів, усі юридичні та фізичні особи, організації, установи та підприємства (а також їх працівники), послугами яких користується ТОВ «МІРОПЛАСТ» для отримання, використання, передачі та знищення ресурсів.

Для кожного ресурсу ТОВ «МІРОПЛАСТ» визначає можливі ризики інформаційної безпеки та шляхи їх мінімізації, тобто компанія використовує ризик-орієнтований підхід, що забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності.

Увесь найманий персонал, підрядники та користувачі третьої сторони повертають всі отримані від ТОВ «МІРОПЛАСТ» ресурси, що перебувають у їх розпорядженні, після припинення їх найму, контракту чи угоди.

Перегляд Політики з інформаційної безпеки ТОВ «МІРОПЛАСТ» здійснюється за потреби, але не менш ніж раз на рік, під час перегляду СУІБ керівництвом компанії.

Слід зазначити, що питання розробки системи управління інформаційною безпекою в компанії є концептуальним. Протягом 2016-2017рр. ТОВ «МІРОПЛАСТ» впровадило Стандарт ISO 27001, що визначає інформаційну безпеку як: «збереження конфіденційності, цілісності та доступності інформації». ISO 27001:2005 являє собою перелік вимог до системи менеджменту інформаційної безпеки, обов'язкових для сертифікації, а стандарт ISO 27002:2005 виступає в якості керівництва по впровадженню, яке може використовуватися при проектуванні механізмів контролю, вибраних організацією для зменшення ризиків інформаційної безпеки. Стандарт ISO 27001 визначає процеси, що представляють можливість бізнесу

встановлювати, застосовувати, переглядати, контролювати і підтримувати ефективну систему менеджменту інформаційної безпеки; встановлює вимоги до розробки, впровадження, функціонуванню, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки в контексті існуючих бізнес ризиків організації.

Процеси управління і забезпечення ІБ наведені на рис.2.9.



Рисунок 2.9 - Процеси управління і забезпечення ІБ

Система управління інформаційною безпекою на основі стандарту ISO 27001 дозволяє: зробити більшість інформаційних активів найбільш зрозумілими для менеджменту компанії; виявляти основні загрози безпеки для існуючих бізнес-процесів; розраховувати ризики і приймати рішення на основі бізнес цілей компанії; забезпечити ефективне управління системою в критичних ситуаціях; проводити процес виконання політики безпеки (знаходити і виправляти слабкі місця в системі інформаційної безпеки); чітко визначити особисту відповідальність; досягти зниження і оптимізації

вартості підтримки системи безпеки; полегшити інтеграцію підсистеми безпеки в бізнес-процеси і інтеграцію з ISO 9001:2000; продемонструвати клієнтам, партнерам, власникам бізнесу свою прихильність до інформаційної безпеки; отримати міжнародне визнання і підвищення авторитету ТОВ «МІРОПЛАСТ», як на внутрішньому ринку, так і на зовнішніх ринках; підкреслити прозорість і чистоту бізнесу перед законом завдяки відповідності стандарту.

Поряд з елементами управління для комп'ютерів і комп'ютерних мереж, стандарт приділяє велику увагу питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпечення безперервності виробничого процесу, юридичним вимогам. Стандарт ISO 27001 гармонізований зі стандартами систем менеджменту якості ISO 9001:2000. За стандартом ISO 27001:2005 проводиться міжнародна сертифікація системи управління інформаційною безпекою та дозволяє наочно показати діловим партнерам, інвесторам і клієнтам, що в компанії захист інформації поставлено на високий рівень і налагоджено ефективне управління інформаційною безпекою.

Згідно із методологією ISF (Information Security Forum) [] нами було оцінено рівень інформаційної безпеки підприємства.

Оцінці підлягають 21 процес ІБ, описаний з урахуванням найбільш відомої міжнародної практики та загальноприйнятих стандартів (ISO27000 і ін.) [27, с. 175] (табл. 2.12, 2.13).

Критерії оцінки рівня зрілості процесів менеджменту ІБ наведені в табл. 2.12.

Таблиця 2.12 – Критерії оцінки рівня зрілості процесів менеджменту ІБ

Рівень зрілості	Позначення рівня зрілості	Опис
0	неіснуючий	Процес ІБ не виконується

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

Таблиця 2.13 - Оцінка рівня зрілості процесів інформаційної безпеки (ІБ) ТОВ «МІРОПЛАСТ»

№	Найменування процесу ІБ	Рівень зрілості
1	Стратегія ІБ	4
2	Усвідомлення керівництвом важливості ІБ	5
3	Управління ризиками ІБ	4
4	Управління комплаєнсом	3
5	Аудит ІБ	4
6	Політика ІБ	4
7	Управління доступом	1
8	Управління уразливими місцями	3
9	Управління ЖЦ АС	3
10	Управління інформаційними активами	3
11	Управління змінами	4
12	Архітектура ІБ	3
13	Управління каналами зв'язку	3
14	Управління зовнішню взаємодією	4
15	Розвідка загроз ІБ	4
16	управління подіями ІБ	4
17	управління інцидентами ІБ	4
18	Антикризове управління	4
19	Забезпечення безперервності бізнесу	5
20	Підвищення обізнаності персоналу	5
21	Безпека персоналу	5
	Загальний рівень зрілості процесів ІБ	3,76

В результаті оцінка рівня зрілості процесів інформаційної безпеки (ІБ) дорівнює: 3,76 – формалізований рівень, що свідчить про те що процес управління ІБ виконується, планується, і є достатній обсяг організаційних ресурсів для підтримки та управління інформаційною безпекою та він не є досконалим.

Розглянемо більш детально основні показники інформаційної складової безпеки ТОВ «МІРОПЛАСТ»:

Продуктивність інформації (PI) (2.1)

$$PI = Bi/V_{\Pi} \quad (2.1)$$

де V_{Π} - обсяг промислової продукції, грн.;

Bi - витрати на придбання інформаційних ресурсів, грн. [39]

Нормативне значення коефіцієнту дорівнює 0,2.

$$PI_{2019} = 11088,7 / 950925,5 = 0,011$$

$$PI_{2020} = 26004,3 / 1078326,9 = 0,024$$

$$V_{\Pi} 2019 \text{ р.} = 950925,5 \text{ тис.грн.}$$

$$V_{\Pi} 2020 \text{ р.} = 1078327 \text{ тис.грн.}$$

$$Bi_{2019} \text{ р.} = 11088,7 \text{ тис.грн.}$$

$$Bi_{2020} \text{ р.} = 26004,3 \text{ тис.грн.}$$

Продуктивність інформації (PI) протягом 2019-2020 рр. була на рівні нижче нормативного та показує наскільки продукція підприємства покриває витрати на забезпечення з отримання інформаційних ресурсів, тобто для того, щоб отримувати необхідну інформацію для повноцінного функціонування, підприємство витрачає фінансові ресурси, щоб забезпечити діяльність інформаційними.

Коефіцієнт інформаційної озброєності KOI (2.2) [27]:

$$KOI = Bi_{\text{р}} / Ч_{\text{сп}}, \quad (2.2)$$

де $Bi_{\text{р}}$ - витрати на придбання інформаційних ресурсів, грн;

$Ч_{\text{сп}}$ - середньоспискова чисельність працівників, чол.

Нормативне значення коефіцієнту $>0,2$

$$\text{КОІ } 2019 = 11088,7 / 600 = 18,48$$

$$\text{КОІ } 2020 = 26004,3 / 597 = 43,55$$

Коефіцієнт інформаційної озброєності (КОІ) показує ступінь озброєності інформацією всього персоналу підприємства та свідчить про те, що протягом 2019-2020рр. ступінь озброєності інформацією персоналу ТОВ «МІРОПЛАСТ» була високою.

Коефіцієнт захищеності інформації (2.3):

$$K3I = B_3 / B_{п}, \quad (2.3)$$

де B_3 - витрати підприємства на захист інформаційних ресурсів, грн;

$B_{п}$ - витрати на придбання інформаційних ресурсів, грн.

Нормативне значення дорівнює 0,1.

$$K3I \text{ } 2019 = 189,56 / 11088,7 = 0,017$$

$$K3I \text{ } 2020 = 598,2 / 26004,3 = 0,023$$

Коефіцієнт захищеності інформації (K3I) показує наскільки є можливість у підприємства забезпечувати діяльність інформаційними ресурсами та їх захист.

Розрахунок показників оцінки інформаційної безпеки свідчить про те, що незважаючи на деяке покращення рівня захищеності інформації на підприємстві в 2020 р. (на 0,006) рівень показника K3I складає 0,023, що не відповідає нормативному значенню – 0,1. Керівництву потрібно вкладати більш фінансових ресурсів для захисту інформаційних ресурсів.

Коефіцієнт інформаційної озброєності (КОІ) за період 2019-2020 рр. збільшився на 25,07 та склав на кінець 2020 р. - 43,55, що вказує на високу ступінь озброєності інформацією всього персоналу підприємства.

Не зважаючи на деяке збільшення протягом 2019-2020 рр. показника продуктивності інформації 0,013 на кінець 2020р. він склав 0,024, що нижче

нормативного показника 0,2 та показує, що продукція підприємства не покриває витрати на забезпечення з отримання інформаційних ресурсів.

Таким чином, в результаті аналізу системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ» було визначено наступне:

Основним завданням системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ» є захист інформаційних ресурсів компанії від зовнішніх та внутрішніх, навмисних та ненавмисних загроз.

Політика інформаційної безпеки ТОВ «МІРОПЛАСТ» описує та регламентує функціонування системи управління інформаційною безпекою відповідно до національних стандартів України з питань інформаційної безпеки ДСТУ ІБО/ІЕС 27000:2015 Інформаційні технології.

Метою Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ», яка буде забезпечувати створення та постійну підтримку умов, при яких ризики, пов'язані з забезпеченням безпеки інформаційних активів компанії, постійно контролюються та знаходяться на прийнятному рівні.

Результати оцінки рівня зрілості процесів інформаційної безпеки (ІБ) свідчать про те, що управління інформаційною безпекою компанії не є досконалим, а система інформаційної безпеки має вразливі місця: слабкість окремих ресурсів СУІБ, якою можуть скористатися одна або більше загроз, (зокрема збій в системі безпеки, який збільшує імовірність реалізації загрози порушення конфіденційності, цілісності, доступності та спостережності інформації).

За результатами проведеного дослідження нами було оцінено загрози ІБ підприємства та виявлено їх вплив на результати діяльності (табл. 2.14).

Таблиця 2.14 – Аналіз впливу загроз ІБ на результати діяльності підприємства

Вид загрози	Опис	Рівень ризику
Стан джерела загрози	в самій системі, що призводить до помилок в роботі і збоїв при реалізації ресурсів АС; в межах видимості АС, наприклад, застосування підслуховуючої апаратури, викрадення інформації в роздрукованому вигляді або крадіжка записів з носіїв даних; шахрайство поза зоною дії АС. Випадки, коли інформація захоплюється під час проходження по шляхах зв'язку, побічний захоплення з акустичних або електромагнітних пристроїв.	середній
Ступінь впливу	активна загроза безпеки, яка вносить корективи в структуру системи і її сутність, наприклад, використання шкідливих вірусів; пасивна загроза - той різновид загрози, яка просто краде інформацію способом копіювання, іноді прихована. Вона не вносить своїх змін в інформаційну систему.	середній
Можливість доступу співробітників до системи програм або ресурсів	шкідливий вплив, то є загроза інформаційним даними може реалізуватися на кроці доступу до системи (несанкціонованого); шкода завдається після згоди доступу до ресурсів системи.	високий
Спосіб доступу до основних ресурсів системи	застосування нестандартного каналу шляху до ресурсів, що включає в себе несанкціоноване використання можливостей операційної системи; використання стандартного каналу для відкриття доступу до ресурсів, наприклад, незаконне отримання паролів і інших параметрів з подальшою маскуванням під зареєстрованого в системі користувача.	високий
Розміщення інформації в системі	вид погроз доступу до інформації, яка розташовується на зовнішніх пристроях пам'яті, начебто несанкціонованого копіювання інформації з жорсткого диска; отримання доступу до інформації, яка показується терміналу, наприклад, запис з відеокамер терміналів; незаконне проникнення в канали зв'язку і підключення до них з метою отримання конфіденційної інформації або для підміни реально існуючих фактів під виглядом зареєстрованого співробітника. Можливо поширення дезінформації; прохід до системної області з боку прикладних програм і зчитування всієї інформації.	високий

Отже, згідно із проведеним дослідженням, нами було виявлено слабкі місця в інформаційної безпеці компанії та визначено рівень ризику від загроз порушення інформаційної безпеки. Порушення інформаційної безпеки може привести до збитків підприємства.

РОЗДІЛ 3 ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

3.1 Заходи із вдосконалення інформаційною безпекою ТОВ «МІРОПЛАСТ»

Побудова ефективної системи управління інформаційною безпекою підприємства - це не разовий проект, а комплексний процес, наплавлений на мінімізацію зовнішніх і внутрішніх загроз при обліку обмежень на ресурси і час.

Для побудови ефективної системи інформаційної безпеки необхідно спочатку описати процеси діяльності, а потім слід визначити поріг ризику - рівень загрози, при якому вона потрапляє в процес управління ризиками. Потрібно побудувати таку систему інформаційної безпеки, яка забезпечить досягнення заданого рівня ризику. Для покращення системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ» нами було розроблено модель процесу управління ризиками для системи інформаційної безпеки підприємства (рис.3.1)

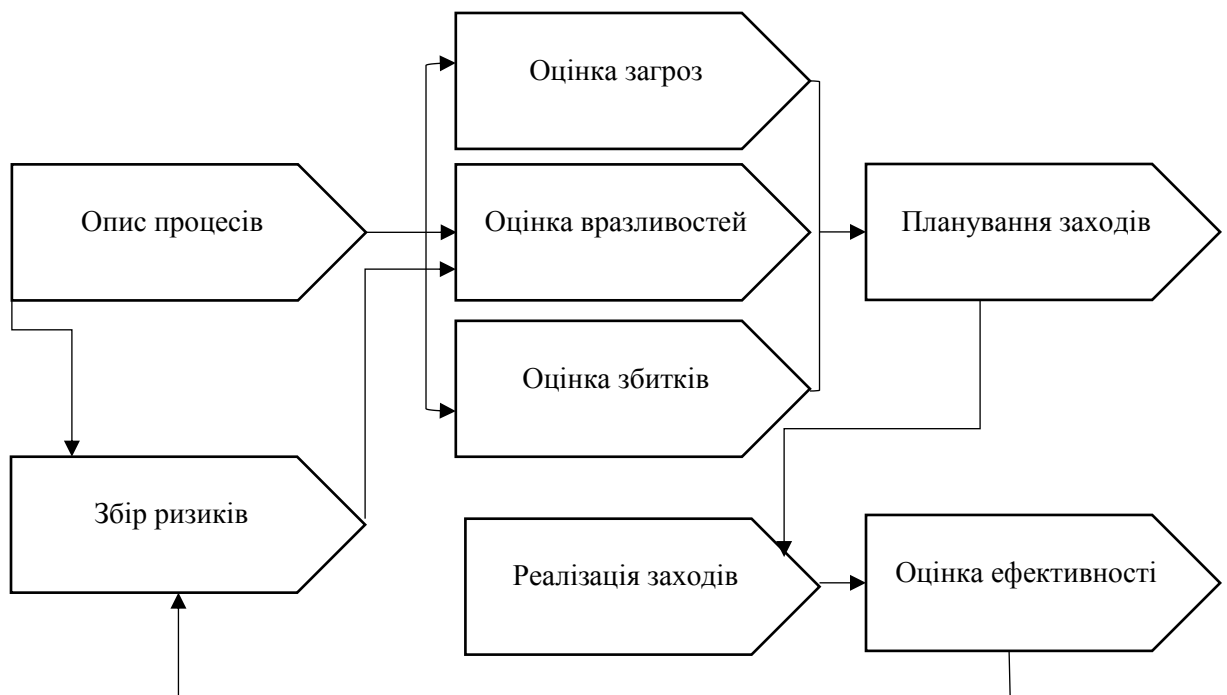


Рисунок 3.1 - Модель процесу управління ризиками для системи інформаційної безпеки ТОВ «МІРОПЛАСТ»

З точки зору процесного підходу систему інформаційної безпеки підприємства можна уявити як процес управління ризиками. На рисунку 3.1 прямокутниками показані узагальнені процеси верхнього рівня, а стрілками показані їх входи і виходи.

Мета будь-якого бізнес-процесу полягає в створенні виходу для отримання винагороди у вигляді іншого виходу. В даному випадку виходом є виключення настання ризикової ситуації або мінімізація її наслідків, а винагородою - збереження матеріальних і фінансових ресурсів.

Серед основних загроз інформаційної безпеки ТОВ «МІРОПЛАСТ» в результаті аналізу були виділені загрози, пов'язані з несанкціонованим доступом до інформації (НСД) - несанкціонований доступ до автоматизованого робочого місця (АРМ) співробітників.

Даний тип загрози характеризується: відсутністю регламенту доступу до АРМ, відсутністю відеоспостереження, відсутністю засобів захисту від несанкціонованого доступу.

До основних організаційних заходів щодо вдосконалення інформаційної безпеки належать:

- організація режиму і охорони. Їх мета - виключення можливості таємного проникнення на територію і в приміщення сторонніх осіб;
- організація роботи зі співробітниками, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення зі співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін.;
- організація роботи з документами та документованою інформацією, включаючи організацію розробки і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення;
- організація використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації;

- організація роботи з аналізу внутрішніх і зовнішніх загроз конфіденційної інформації та вироблення заходів щодо забезпечення її захисту;

- організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів і технічних носіїв.

У кожному конкретному випадку організаційні заходи носять специфічну для даної організації форму і зміст, спрямовані на забезпечення безпеки інформації в конкретних умовах.

Для усунення даного типу загроз нами було запропоновано наступне:

- 1 Впровадити на об'єкт відеоспостереження, яке буде призначене для контролю співробітників, що мають доступ до інформації обмеженого доступу, а також для виявлення несанкціонованого проникнення в приміщення з конфіденційною інформацією.

- 2 Необхідно встановити спеціальний програмно-апаратний засіб захисту інформації.

Нами було розроблено проект заходів щодо підвищення ефективності управління інформаційною безпекою ТОВ «МІРОПЛАСТ» (табл.3.1)

Охарактеризуємо кожен етап реалізації проекту:

- 1 Впровадження системи контролю і управління доступом (СКУД) на базі технологій Cisco.

- 2 Закупка і установка системи відеоспостереження

Загальна вартість проекту заходів щодо підвищення ефективності управління інформаційною безпекою ТОВ «МІРОПЛАСТ» складає 915,00 тис.грн.

Система інформаційної безпеки Cisco Stealthwatch забезпечує надійний захист периметра мережі та моніторинг в рамках всієї мережі, ЦОД та хмари й виявляє приховані атаки за допомогою розширених функцій аналітики безпеки. Система складається з наступних блоків:

Таблиця 3.1 - Проект заходів щодо підвищення ефективності управління інформаційною безпекою ТОВ «МІРОПЛАСТ»

№	Захід	Строк виконання	Відповідальна особа	Планована вартість, тис.грн
	1	2	3	4
1	Система контролю і управління доступом (СКУД) на базі технологій Cisco Stealthwatch	червень – грудень 2021р	Директор з інформаційної безпеки	580,00
2	Система відеоспостереження:	липень-серпень 2021р.	Начальник служби безпеки	335,00
3	SIP сервер Dahua VTSS5000			225,00
4	Комплект IP відеоспостереження CoVi Security NVK-4001 IP KIT			110,00
	Всього			915,00

1 Advanced Malware Protection - розширений захист від шкідливих програм

2 ETA_icon - аналіз зашифрованого трафіку

3 Advanced Malware Protection (AMP) - забезпечує моніторинг і контроль для швидкого виявлення, стримування та усунення шкідливого ПЗ.

4 Firepower 2100 series - включає функції моніторингу і контролю додатків (AVC), систему запобігання вторгнень нового покоління (NGIPS), захист від складного шкідливого ПЗ (Cisco AMP) і фільтрацію URL-адрес.

5 Esa-large Email Security Appliance (ESA) - надає захист від зростаючої кількості загроз електронної пошти: спаму, фішингу, шкідливого коду і витоків інформації.

Впровадження рішень Cisco (Web Security Appliance і Email Security Appliance) проводиться без переривання роботи сервісів і з мінімальним впливом на діяльність користувачів.

Введення в експлуатацію рішення для віддаленого доступу до внутрішніх сервісів компанії співробітників і зовнішніх партнерів на основі міжмережових екранів Cisco ASA 5555 і серверів авторизації Cisco Identity Service Engine (ISE) надасть можливість отримати безпечний доступ до корпоративних ресурсів. Впровадження дозволить користуватися

інструментами, що знаходяться усередині мережі, мінімізуючи ризики несанкціонованого доступу. За допомогою сервісу реалізується функція контролю налаштувань робочих станцій для відповідності вимогам безпеки банку.

Рішення Cisco ASA з сервісами FirePower підвищує рівень захищеності компанії і надає нові можливості ретроспективного аналізу.

В ІБ-інфраструктурі включено рішення Cisco Advanced Malware Protection для кінцевих пристроїв (AMP for Endpoints), що використовує технологію запобігання атак наступного покоління. Агенти AMP встановлюються як додатковий захід захисту на кінцевих точках разом з антивірусними програмами. Рішення AMP for Endpoints грає ключову роль в запобіганні деяких атак, що пройшли зовнішню лінію оборони.

Архітектура Cisco SAFE забезпечує узгодженість інструментів і дозволяє вирішувати операційні завдання на всьому життєвому циклі атаки - до, під час і після. Системи успішно функціонують і забезпечують безпечний доступ в Інтернет і корпоративну мережу компанії, поштовий обмін для всіх співробітників. Фахівці можуть безпечно взаємодіяти з зовнішніми контрагентами.

Спам-фільтри, захист електронної пошти, захист периметра від мережеских погроз - неповний список вирішених системою завдань. Блок аналізу мережевого трафіку Cisco StealthWatch встановлено для того, щоб оперативно отримувати інформацію про джерела і кінцеві об'єкти, що становлять загрозу для підприємства.

Система відстежує рух трафіку, пристрої, які отримують доступ в мережу, а також потенційно шкідливі дії.

Структура системи інформаційної безпеки Cisco Stealthwatch наведена на рис.3.2.

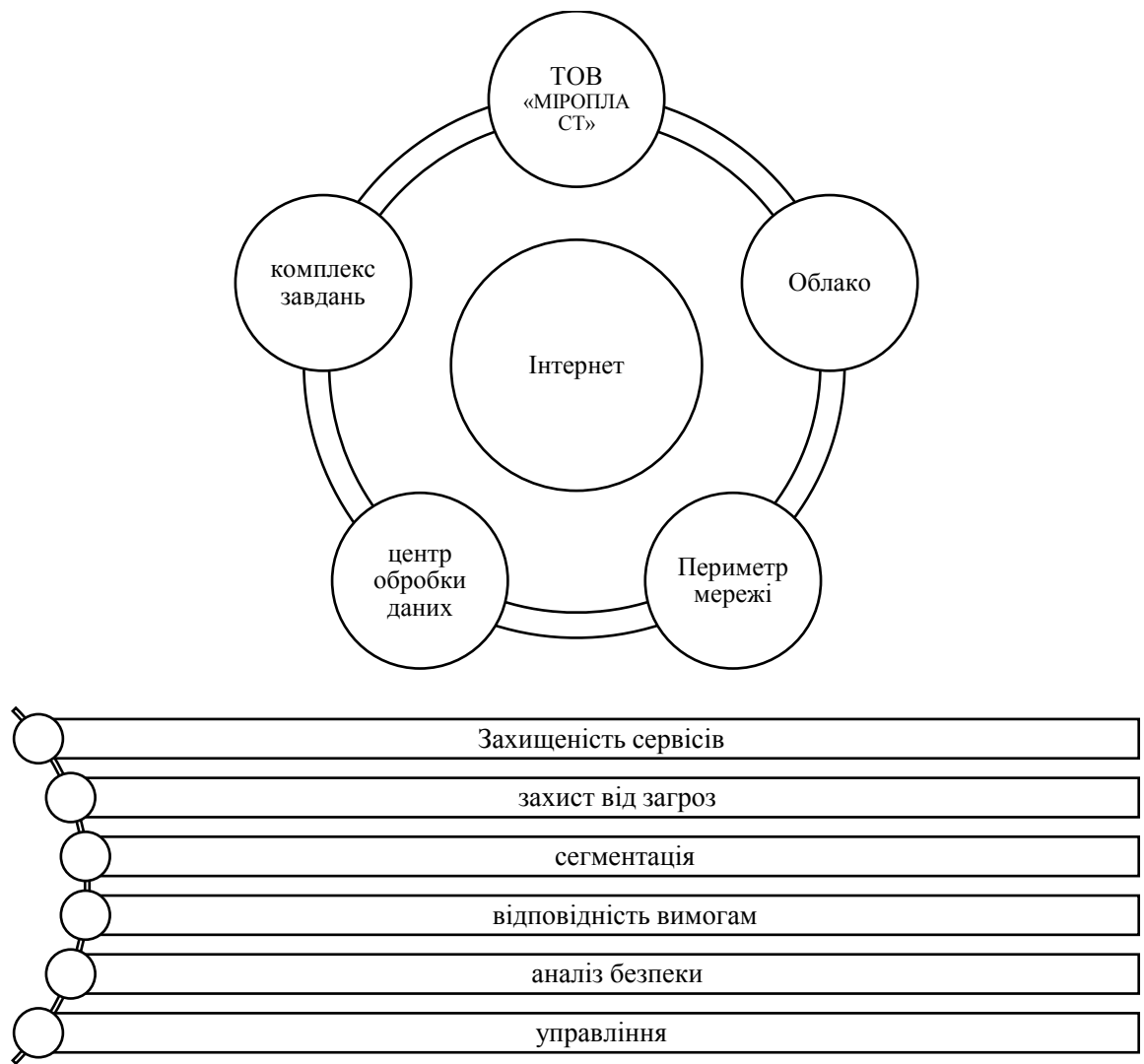


Рисунок 3.2 - Структура системи інформаційної безпеки Cisco Stealthwatch

Система відеоспостереження (відеонагляду, відеоконтролю) призначена для організації отримання інформації про поточний стан об'єкту, що охороняється (технологічного процесу) шляхом збору, обробки, архівування, зберігання, відображення та аналізу цієї інформації. Метою установки системи відеоспостереження є перегляд місць, які важливо контролювати з точки зору збереження матеріальних цінностей, контролю за проникненням на об'єкт (прохідні, паркани, двері, ворота і ін.), стеження за переміщенням об'єктів.

Система відеоспостереження на підприємстві дозволяє забезпечити потрібний рівень захисту і безпеки як персоналу, так і майна підприємства.

Охоронне відеоспостереження на підприємстві ТОВ «МІРОПЛАСТ» повинно стати невід'ємною частиною системи безпеки такого об'єкта.

Установка відеоспостереження на підприємстві дуже важлива. Так як кількість працівників ТОВ «МІРОПЛАСТ» досягає 600 осіб, то забезпечення їх безпеки та безпеки підприємства займає головне місце адже дуже важливим є своєчасне реагування на будь-які загрози.

Виходячи з цього, ми рекомендуємо керівництву підприємств встановити охоронне внутрішнє та зовнішнє відеоспостереження. Зовнішнє відеоспостереження на підприємстві дозволяє вести відеоконтроль відкритої території підприємства. Так за допомогою вуличного відеоспостереження на підприємстві можна організувати контроль доступу центрального входу, а також забезпечити своєчасне реагування на будь-які зовнішні загрози.

Внутрішнє відеоспостереження покликане забезпечувати постійний контроль того, що відбувається всередині організації.

Якщо розглядати виробниче підприємство ТОВ «МІРОПЛАСТ», то на таких об'єктах відеоспостереження часто використовується для контролю виробничого процесу та забезпечення інформаційної безпеки на підприємстві. Сучасні багатофункціональні відеокамери здатні фіксувати всі дрібні дії і надавати деталізоване відео. Для організації відеоспостереження на підприємстві необхідно визначити всі функціональні зони і необхідні відеокамери для виконання завдань у цих зонах. Так якщо ми розглядаємо офіс компанії, то відеокамери повинні забезпечувати дії робітників. За допомогою відеоспостереження можна миттєво побачити появу різних загроз і оперативно відреагувати на них.

Система відеоспостереження підприємств створює можливість контролювати персонал і відвідувачів об'єкта.

Система відеоспостереження підприємства в цілому в рази підвищує ефективність роботи самого підприємства та суттєво впливає на продуктивність персоналу.

3.2 Оцінка ефективності запропонованих заходів

Розрахунок потреби в інвестиціях на реалізацію Проекту підвищення ефективності управління інформаційною безпекою ТОВ «МІРОПЛАСТ» наведено в табл.3.2.

Таблиця 3.2 - Розрахунок потреби в інвестиціях

№	Вид	Тип, марка	Кількість	Ціна один. (тис.грн.)	Сума (тис. грн.)
1	Система контролю і управління доступом (СКУД)	Cisco Stealthwatch	1	580,00	580,00
2	Система відеоспостереження	Elsy	1	335,00	335,00
3	SIP сервер	Dahua VTSS5000	1	225,00	225,00
4	Комплект IP відеоспостереження	CoVi Security NVK-4001 IP KIT	1	110,00	110,00
	Всього				915,00

З урахуванням цих вкладень потреба в інвестиційних ресурсах на реалізацію Проекту підвищення ефективності управління інформаційною безпекою ТОВ «МІРОПЛАСТ» складає 915,00 тис.грн. Дане вкладення є разовим та включає в свою вартість монтаж обладнання та навчання персоналу роботі з ним, що закріплено в пункті договору постачання.

Джерела інвестування – власні фінансові ресурси в сумі 915,00 тис.грн. (табл.3.3).

Таблиця 3.3 - Джерела інвестування

Джерела інвестування	тис.грн.	питома вага (%)
Власні кошти	915,00	100,00
Позикові кошти	0,00	0,00

Основними внутрішнім джерелом фінансування Проекту підвищення ефективності управління інформаційною безпекою ТОВ «МІРОПЛАСТ» є чистий прибуток компанії. Отже, в структурі джерел інвестування проекту 100% займають власні кошти компанії.

Одним з найбільш поширених методів оцінки ефективності вкладень є метод розрахунку чистої приведеної вартості, Net present value - NPV або ЧДД) (табл. 3.4, рис. 3.3). Net Present Value (NPV, чистий дисконтований дохід) - один з найпоширеніших показників ефективності інвестиційного проекту. Це різниця між дисконтованими за часом надходженнями від проекту та інвестиційними витратами на нього.

Таблиця 3.4 – Оцінка ефективності проекту вдосконалення інформаційної безпеки ТОВ «МІРОПЛАСТ»

Період	0	2021р	2022р	2023р	Ітого
Грошовий потік	-915,00	190,00	450,00	450,00	175,00
Ставка дисконтування	7,50%				
Чистий дисконтований дохід (NPV)	-915,00	176,74	389,40	362,23	13,38
	13,38	13,38	175,00		
Внутрішня норма доходності (IRR)	8,21%				

Ставка дисконту - це відсоткова ставка, яка застосовується до майбутніх доходів і враховує ризик та невизначеність, пов'язані з фактором часу.

Ставка дисконтування складається з трьох складових:

- відсоткова ставка на позикові кошти – це та винагорода, яку отримав би кредитор, якби надав у користування на певний строк певну суму коштів;
- відсоткова ставка кредитного ризику – ризик, який враховує кредитор у разі неповернення позиченої суми;
- очікувана процентна ставка інфляції.

В якості більших гарантій отримання доходу у майбутньому можна використовувати кумулятивний метод визначення ставки дисконтування. Він оцінює вплив факторів ризику на заплановані грошові потоки [25]

$$r = r_f + r_p + I, \quad (3.1)$$

де r_f - безризикова ставка = 1,5%

gr - премія за ризик = 0,5%

I - відсоток інфляції: в 2020 р. – 5,5%

$r = 1,5 + 0,5 + 5,5 = 7,5\%$

Фінансовими аналітиками обирається ставка дисконтування у відповідності до потреб зацікавлених осіб. Єдиної вірної ставки дисконтування не існує, однак використовується ключове інвестиційне правило: "Ставка дисконту повинна бути більшою, ніж безризикові інвестиції".

Облікова ставка НБУ, або ставка рефінансування - процентна ставка, що стягується Національним банком України під час рефінансування комерційних банків. Це монетарний інструмент, за допомогою якого Нацбанк встановлює для суб'єктів грошово-кредитного ринку орієнтир щодо вартості залучених та розміщених грошових ресурсів. з 16.04.2021 вона становить - 7,5% (<https://index.minfin.com.ua/banks/nbu/refinance/>)

За відсутності ринкової ставки відсотка ставка дисконту базується на ставці відсотка на можливі позики підприємства або розраховується за методом середньозваженої вартості капіталу підприємства.

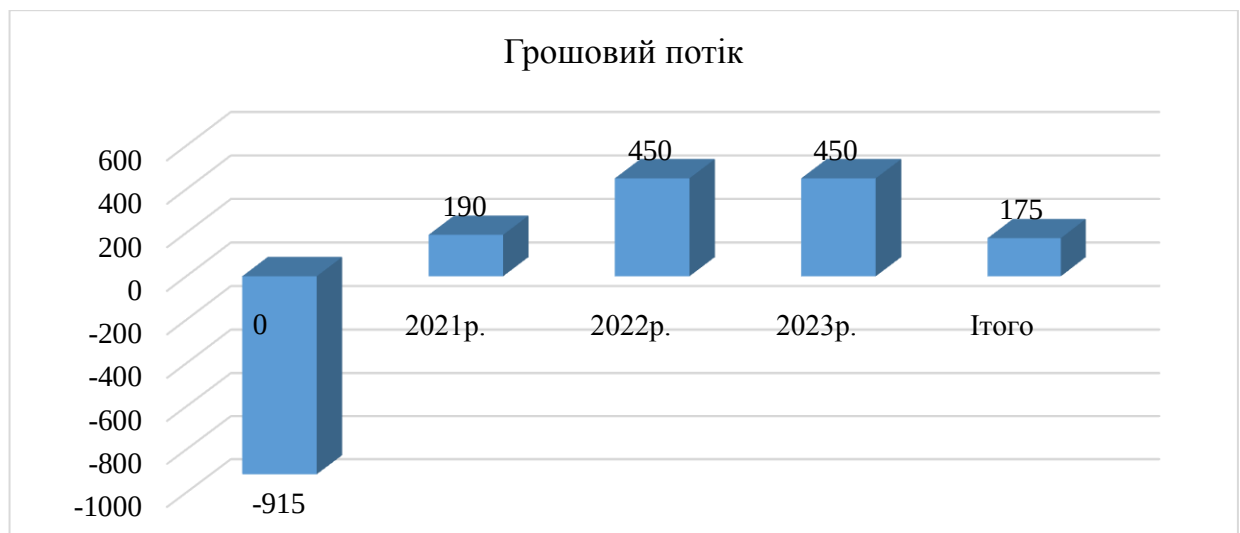


Рисунок 3.3 – Грошовий потік за проектом

Так як NPV проекту склав $13,38 > 0$ - проект є економічно ефективним. Внутрішня норма прибутковості (IRR) становить 8,21%. Індекс прибутковості інвестицій ($Profitability\ index, PI$) ілюструє ставлення віддачі

капіталу до розміру вкладеного капіталу, показник прибутковості інвестицій показує відносну прибутковість проекту в розрахунку на одиницю вкладень. Індекс прибутковості розраховується за формулою [25]:

$$PI = NPV / I \quad (3.2)$$

де I - вкладення;

$$PI = 13,38 / 915,00 = 1,46\%.$$

Так як $PI = 1,46\% > 0$ вкладення в проект рентабельні і прийнятні відповідно до обраної ставкою дисконтування. Реалізація запропонованих заходів сприятиме підвищенню рівня інформаційної безпеки компанії і ефективності роботи в цілому.

Строк окупності (Payback Period, PP) проекту - це період, що потрібен для того, щоб були повністю відшкодовані початкові інвестиції, вкладені в проект. Тобто це той період, після якого початкові вкладення почнуть генерувати стабільний грошовий потік і дозволять інвестору отримувати прибуток.

Розрахуємо строк окупності проекту за формулою (3.3) [25]:

$$PP = IC / CF, \quad (3.3)$$

де PP (Pay-Back Period) - простий термін окупності, виражений в роках / місяцях;

$IC=915$ тис.грн. (Invest Capital) - сума початкових інвестицій;

$CF=363,33$ тис.грн. (Cash Flow) - очікуваний середньорічний грошовий потік.

$$PP = 915,00 / 363,33 = 2,51 \text{ років}$$

Далі для оцінки проекту підвищення ефективності системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ» нами було розраховане прогнозований рівень зрілості процесів інформаційної безпеки (ІБ) (табл. 3.5).

Таблиця 3.5 – Прогноз змін рівня зрілості інформаційної безпеки (ІБ)
ТОВ «МІРОПЛАСТ»

№	Найменування процесу ІБ	Рівень зрілості	Прогнозований рівень зрілості	Зміни (+/-)
1	Стратегія ІБ	4	5	1
2	Усвідомлення керівництвом важливості ІБ	5	5	0
3	Управління ризиками ІБ	4	5	1
4	Управління комплаєнсом	3	4	1
5	Аудит ІБ	4	4	0
6	Політика ІБ	4	4	0
7	Управління доступом	1	5	4
8	Управління уразливими місцями	3	5	2
9	Управління ЖЦ АС	3	3	0
10	Управління інформаційними активами	3	4	1
11	Управління змінами	4	4	0
12	Архітектура ІБ	3	5	2
13	Управління каналами зв'язку	3	4	1
14	Управління зовнішньою взаємодією	4	4	0
15	Розвідка загроз ІБ	4	5	1
16	управління подіями ІБ	4	5	1
17	управління інцидентами ІБ	4	5	1
18	Антикризове управління	4	4	0
19	Забезпечення безперервності бізнесу	5	5	0
20	Підвищення обізнаності персоналу	5	5	0
21	Безпека персоналу	5	5	0
	Загальний рівень зрілості процесів ІБ	3,76	4,52	+0,76

В результаті, рівень зрілості процесів інформаційної безпеки (ІБ) до реалізації запропонованих заходів щодо покращення системи управління інформаційною безпекою дорівнював: 3,76 – формалізований рівень, що свідчить про те що процес управління ІБ виконується, планується, і є достатній обсяг організаційних ресурсів для підтримки та управління інформаційною безпекою та він не є досконалим. Після реалізації програми вдосконалення управління інформаційною безпекою ТОВ «МІРОПЛАСТ» прогнозується значне покращення показника до рівня 4,52 – керований рівень, це свідчить про те, що процес ІБ виконується, планується, керується і контролюється.

Прогнозована зміна показників інформаційної складової безпеки підприємства наведена в табл.3.6.

Таблиця 3.6 – Прогнозована зміна показників інформаційної складової безпеки ТОВ «МІРОПЛАСТ»

Показник	2019р	2020р	Прогноз	Зміна, прогноз/2020 р. (+/-)
Продуктивність інформації (PI)	0,01	0,02	0,03	0,01
Коефіцієнт інформаційної озброєності КОІ	18,48	43,56	47,54	3,98
Коефіцієнт захищеності інформації (КЗІ)	0,018	0,023	0,126	0,103

Отже, після впровадження пропозицій прогнозується покращення всіх показників інформаційної складової безпеки ТОВ «МІРОПЛАСТ», а саме: коефіцієнту захищеності інформації більш ніж у два рази (рис.3.4).

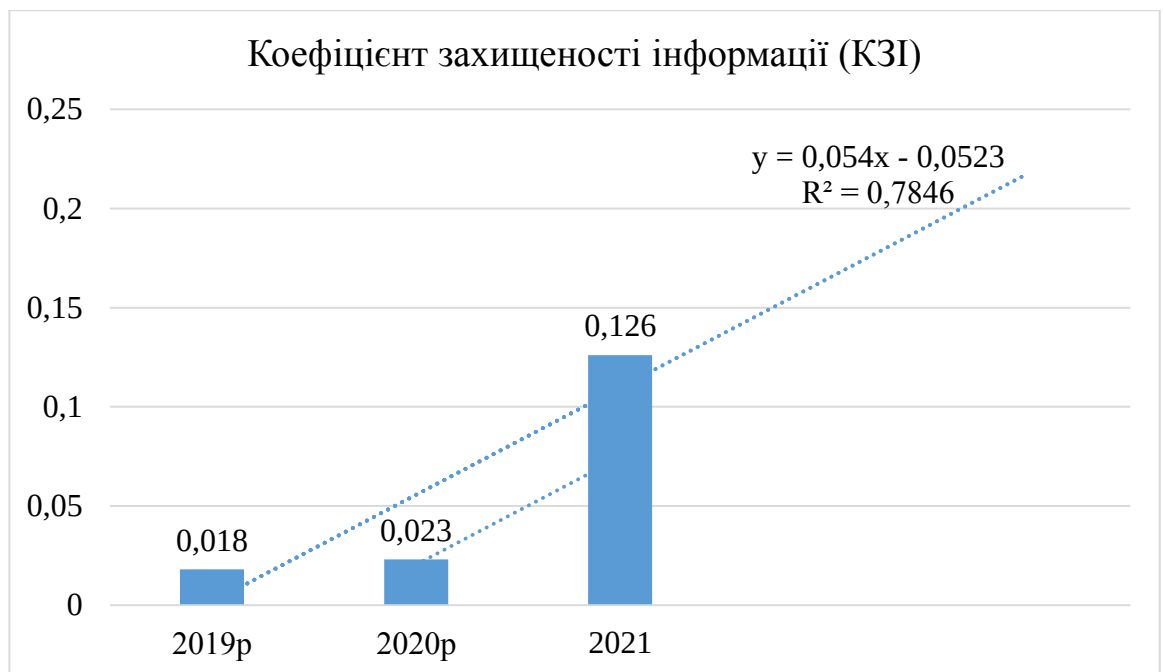


Рисунок 3.4. - Прогноз зростання коефіцієнту захищеності інформації

В результаті впровадження проекту завдяки до збільшення витрат підприємства на захист інформаційних ресурсів прогнозується значне покращення рівня інформаційної безпеки та його гармонізація до нормативного значення $\geq 0,1$.

Підсумкові показники ефективності проекту наведені в табл. 3.7.

Таблиця 3.7 - Підсумкові показники ефективності проекту підвищення ефективності управління інформаційною безпекою на ТОВ «МІРОПЛАСТ»

Показник	Значення
Рівень зрілості процесів інформаційної безпеки	4,52
Коефіцієнт захищеності інформації (КЗІ)	0,126
Чиста поточна вартість (NPV) при ставці дисконтування 7,5%	13,38
Внутрішня норма доходу (рентабельності) на інвестиції (IRR)	8,21%.
Період окупності (payback period)	2,51 роки
Індекс прибутковості інвестицій	1,46%

Результати розрахунку економічної ефективності проекту вдосконалення управління інформаційної безпеки на ТОВ «МІРОПЛАСТ» свідчать про те, що проект є рентабельним. Реалізація запропонованих заходів сприятиме підвищенню рівня організації роботи щодо покращення управління інформаційною безпекою компанії, а також загальному зростанню ефективності роботи ТОВ «МІРОПЛАСТ» в цілому.

ВИСНОВКИ

Отже, в результаті проведеного дослідження інформаційної безпеки підприємницької діяльності нами було виконане поставлені завдання та отримана можливість для формулювання наступних висновків:

1 Поняття «інформаційна безпека» слід розглядати як стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення.

2 Забезпечення інформаційної безпеки (ІБ) підприємницької діяльності можливо тільки при системному і комплексному підході до захисту. В системі ІБ повинні враховуватися всі актуальні комп'ютерні загрози і вразливості. Повноцінна інформаційна безпека підприємств і організацій повинна здійснювати безперервний контроль в реальному часі всіх важливих подій і станів, що впливають на безпеку даних. Захист повинен здійснюватися цілодобово і цілорічно і охоплювати весь життєвий цикл інформації - від її надходження або створення до знищення або втрати актуальності.

3 Управління інформаційною безпекою підприємницької діяльності є важливим аспектом забезпечення безпеки властивостей інформаційних ресурсів та послуг в мережах передачі даних. Для досягнення й підтримки безпеки в інформаційно-комунікаційних системах та мережах потрібен певний діапазон засобів та заходів управління. На сьогодні існує безліч способів боротьби з загрозами інформаційній безпеці підприємницької діяльності. Для кожної загрози підбираються свої методи і процеси, які контролюють певні вузли інформаційної системи і запобігають будь-якому збою в них. Однак максимального ефекту можна домогтися тільки

застосуванням всіх цих методів в комплексі. Тобто проектування, побудова, впровадження і підтримка системи інформаційної безпеки - це комплексна задача, яка потребує аналізу потенційних загроз, вибору методів боротьби з ними та налагодження взаємодії між цими методами.

4 В результаті аналізу системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ» було визначено наступне:

Основним завданням системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ» є захист інформаційних ресурсів компанії від зовнішніх та внутрішніх, навмисних та ненавмисних загроз.

Політика інформаційної безпеки ТОВ «МІРОПЛАСТ» описує та регламентує функціонування системи управління інформаційною безпекою відповідно до національних стандартів України з питань інформаційної безпеки ДСТУ ІБО/ІЕС 27000:2015 Інформаційні технології.

Метою Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ», яка буде забезпечувати створення та постійну підтримку умов, при яких ризики, пов'язані з забезпеченням безпеки інформаційних активів компанії, постійно контролюються та знаходяться на прийнятному рівні.

Результати оцінки рівня зрілості процесів інформаційної безпеки (ІБ) свідчать про те, що управління інформаційною безпекою компанії не є досконалим, а система інформаційної безпеки має вразливі місця: слабкість окремих ресурсів СУІБ, якою можуть скористатися одна або більше загроз, (зокрема збій в системі безпеки, який збільшує імовірність реалізації загрози порушення конфіденційності, цілісності, доступності та спостережності інформації).

5 Побудова ефективної системи управління інформаційною безпекою підприємства - це не разовий проект, а комплексний процес, наплавлений на мінімізацію зовнішніх і внутрішніх загроз при обліку обмежень на ресурси і час. Для побудови ефективної системи інформаційної безпеки необхідно спочатку описати процеси діяльності, а потім слід визначити поріг ризику -

рівень загрози, при якому вона потрапляє в процес управління ризиками. Потрібно побудувати таку систему інформаційної безпеки, яка забезпечить досягнення заданого рівня ризику. Для покращення системи управління інформаційною безпекою ТОВ «МІРОПЛАСТ» нами було розроблено модель процесу управління ризиками для системи інформаційної безпеки підприємства та розроблені пропозиції щодо вдосконалення.

Результати розрахунку економічної ефективності проекту вдосконалення управління інформаційної безпеки на ТОВ «МІРОПЛАСТ» свідчать про те, що проект є рентабельним. Реалізація запропонованих заходів сприятиме підвищенню рівня організації роботи щодо покращення управління інформаційною безпекою компанії, а також загальному зростанню ефективності роботи ТОВ «МІРОПЛАСТ» в цілому.

БІБЛІОГРАФІЧНИЙ СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про інформацію: Закон України від 02.10.92 № 2658-ХІІ. Дата оновлення: 16.07.2020. URL: zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12 (дата звернення: 06.04.2021)
2. Про захист інформації в інформаційно телекомунікаційних системах: Закон України від 05.07.94 № 81/94-ВР. Дата оновлення: 01.07.2020. URL: zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80%2F94-%E2%F0 (дата звернення: 12.03.2021)
3. Про науково-технічну інформацію: Закон України від 25.06.93 № 3323-ХІІ. Дата оновлення: 19.04.14. URL: zakon2.rada.gov.ua/laws/show/3322-12 (дата звернення: 02.04.2021)
4. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI *Відомості Верховної Ради України*. № 36. 2011. С. 93.
5. Про затвердження Концепції технічного захисту інформації в Україні Постанова Кабінету Міністрів України від 08.10.1997 р. *Офіційний вісник України*. 2018. № 5. С. 430–443.
6. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення. [Чинний від 1997-01-01]. Вид. офіц. Київ, 2015. 16 с. (Інформація та документація).
7. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави: затв. постановою Кабінету Міністрів України від 27.11.98. № 1893. *Офіційний вісник України*, 1998. 12 лип. (№ 48). С. 1764.
8. Про порядок здійснення криптографічного захисту інформації в Україні: наказ Президента України від 22.05.98 р. № 505/98. *Урядовий кур'єр*, 1998. 9 лип. (№33). С. 218.

9. Про затвердження Концепції технічного захисту інформації в Україні: Постанова Кабінету Міністрів України від 8.10.1997 р. № 1126 *Офіційний вісник України*. 2000. №12. С. 1714.
10. Андрианов В.В. Оценка информационной безопасности бизнеса: монография. Москва: ЦИПСИР: Альпина Паблишерз, 2011. 373 с.
11. Березюк Л.П. Организационное обеспечение информационной безопасности: учебное пособие. Хабаровск: ДВГУПС, 2008. 190 с.
12. Богуш В.М., Юдін О.К. Інформаційна безпека держави: монографія. Київ: «МК-Пресс», 2005. 432 с.
13. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства *Управління проектами та розвиток виробництва*. Київ. 2014. №4 (52). С. 28-39.
14. Велігура А.В. Дослідження шляхів розробки комплексів інформаційної безпеки *Вісник Східноукраїнського національного університету імені В.Даля*. Луганськ. 2009. № 6 (136). С 154–161.
15. Войтович О.П., В.А. Лужицький, А.Д. Кожухівський. Основи інформаційної безпеки: навч. посібник. Вінниця: ВНТУ, 2015. 221 с.
16. Вострцова Е.В. Основы информационной безопасности: учебн. пособие. Екатеринбург: Урал, 2019. 204 с
17. Галатенко В.А. Основы информационной безопасности: учебн. пособие. Москва: ИНТУИТ.ру, 2003. 280 с.
18. Голубев В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: монографія. Запоріжжя : Просвіта, 2001. 252 с.
19. Гордієнко С. Г. Теорія та практика діяльності державних та недержавних структур із захисту інтелектуальної власності в Україні в сучасних умовах: курс лекцій. Київ.: НТУУ «КП», 2011. 496 с.
20. Гордієнко С. Б. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії. *Вісник Державного*

університету інформаційно-комунікаційних технологій ДУІКТ. Київ, 2013. № 1. С. 104-107.

21. Гришина Н. В. Организация комплексной системы защиты информации: монография Москва: Гелиос АРВ. 2007. 256 с.

22. Гуцу С.Ф. Правові основи інформаційної діяльності: навч. посібник. Харків: Нац. аерокосм. ун-т «Харк. авіац. ін-т». 2009. 48 с.

23. Дербин Е.А. Организационные основы обеспечения информационной безопасности предприятия: учебн. пособие. Москва: Финансовый университет, 2013. 266 с.

24. Дячков Д. В. Методичні підходи до оцінки інформаційної безпеки підприємства. *Економічні науки*. Київ. 2019. №7. С.32-41.

25. Економіка та менеджмент: збірник наукових праць/ відп. ред. З.В. Герасимчук Луцький державний технічний університет. Луцьк. 2004. Випуск 1. С. 85-109.

26. Живко З. Б. Соціально-економічна безпека: навч. посіб. Львів : Ліга-Прес, 2008. 345 с.

27. Журавель М.Ю. Формування системи показників оцінки рівня інформаційної безпеки підприємства. *Вісник економіки транспорту і промисловості*. Київ, 2011. № 33. С. 171-177.

28. Захаркін О.О., Абрамчук М.А. Інформаційні системи та технології у фінансових установах: монографія. Суми : СумДУ, 2007. 80 с.

29. Зубок М.І. Інформаційна безпека в підприємницькій діяльності : навч. посібник. Київ: ГНОЗІС, 2015. 216 с.

30. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия: монография. Старый Оскол: ООО «ТНТ», 2005. 448 с.

31. Економічний енциклопедичний словник. Інформаційна безпека. URL: zalik.org.ua/index.php (дата звернення: 16.02.2021)

32. Конахович Г.Ф. Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекоммуникационных системах. Київ: «МК-Пресс», 2005. 288 с.
33. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посібник. Київ: Кондор, 2004. 384 с.
34. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література, 2003. 472 с.
35. Корченко О.Г., Дрейс Ю.О. Нормативно-правове забезпечення інформаційної безпеки: збірник нормативно-правових документів. Житомир : ЖВІ НАУ, 2019. 280 с.
36. Кравчук О. Я., Кравчук П.Я. Діагностика рівня та критерії оцінки корпоративної безпеки суб'єктів господарювання. *Економічні науки*. Київ, 2017. №4. С.21-29
37. Крюков О.І. Інформаційна безпека держави в умовах глобалізації *Державне будівництво*. Київ, 2015. № 2. С. 36.
38. Кулініч О. А. Структурні чинники економічної безпеки України *Шлях України до економічної безпеки: матеріали наук.-практ. конф.* Харків: ХНУВС, 2007. С. 59-63.
39. Ленков С.В. Методы и средства защиты информации: монографія. Київ: Арій, 2008. 464 с.
40. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): автореф. дис. на здобуття наук. ступеня канд. політ. наук: спец. 23.00.04/ Нац. авіаційний університет (НАУ). Київ, 1997. 18с.
41. Логінова Н. І. Правовий захист інформації: навч. посібник. Одеса: Фенікс, 2015. 264 с.
42. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие. Москва: Горячая линия – Телеком, 2004. 280 с.

43. Маруніч А. В. Захист інформації як основна складова економічної безпеки підприємства. *Управління розвитком*. Київ, 2014. № 14. С. 130-132.
44. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України*. Київ, 2011. № 21. С. 92-95.
45. Момот А. Аналіз основних напрямків забезпечення інформаційної безпеки *Актуальні проблеми міжнародних відносин*. Київ, 2008. Вип.659 (Ч.1) №1. С.265-278.
46. Низенко Е.І., Каленяк В.П. Забезпечення інформаційної безпеки підприємництва: навч. Посібник. Київ: МАУП, 2006. 134 с.
47. Новиков О.М. Безпека інформаційно-комунікаційних систем: підручник. Київ: ВНУ, 2009. 608 с.
48. Остроухов В.В., Петрик В.М., Кузьменко А.М. Соціально-правові основи інформаційної безпеки: навч. посібник. Київ: Росава, 2017. 496 с.
49. Петрик В.М. Щодо визначення інформаційної безпеки та її різновидів *Форми та методи забезпечення інформаційної безпеки держави: збірник матеріалів міжнародної науково-практичної конференції (м.Київ, 13 березня 2008 р.)*. Київ: Видавець Захаренко, 2008. С. 160–164.
50. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації: навч. посібник. Київ: Вид. Національної академії внутріш. справ, 2012. 104с.
51. Сідак В.С. Організаційно-правові основи захисту інформації з обмеженим доступом: навч. посібник. Київ: Вид-во Європ. ун-ту, 2006. 232 с.
52. Смірнов О.А. Основи захисту інформації: навч. посібник. Кіровоград : РВЛ КНТУ, 2011. 322 с.
53. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи *Вісник Хмельницьк. нац. ун-ту. Сер.: Екон. науки*. 2010. № 2. С. 32–35.

54. Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим): автореф. дис. на здобуття наук ступеня канд. екон. наук: 08.00.04/ Таврический Национальный Университет им. В.И. Вернадского Сімферополь, 2012. 21с.

55. Тихомиров О.О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: мета, засоби і методи, принципи, результати *Information Security of the Person, Society and State*. Київ, 2012. № 3(10). С. 11-17.

56. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки. *Інформація і право: науковий журнал*. – Київ: НДЦП НАПрН України, 2012. № 1(4). С.46– 56.

57. Харченко Л.С., Ліпкан В.А., Логінов О.В. Інформаційна безпека України: глосарій. Київ: Текст, 2004. 136 с.

58. Хорошко В.О. Основи інформаційної безпеки: навч. посібник. Київ: ДУІКТ, 2018. 186 с.

59. Цимбалюк В. Інформаційна безпека підприємницької діяльності, визначення сутності та змісту поняття за умами входження України до інформаційного суспільства (глобальної кіберцивілізації) *Підприємництво, господарство і право*. Київ, 2004. №3 С.88-91

60. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Київ, 2004. №8. С.30–33.

61. Чунарьова А.В. Система управління інформаційною безпекою на базі міжнародних стандартів серії ISO *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: науково-технічний збірник*. Київ: НТУУ КПІ, 2012. № 2(24). С.50-53.

62. Шевченко С.Ю. Формування системи управління інформаційної безпеки підприємства *Економіка підприємства: теорія та практика: збірн.*

матер. IV міжнар. наук.- практ. конф. 12 жовт. 2012р. Київ: КНЕУ, 2012. 482с.

63. Юдін О.К., Корченко О.Г., Коханович Г.Ф. Захист інформації в мережах передачі даних: монографія. Київ: Вид-во DIRECTLINE, 2018. 714 с.

64. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підручник. Київ: НАУ, 2011. 620 с.

65. Ясенов В. Н. Информационная безопасность в экономических системах: учеб. пособ. Н. Новгород: ННГУ, 2006. 308с.

ДОДАТКИ

Додаток 1
до Національного положення (стандарту)
бухгалтерського обліку 1 «Загальні вимоги
до фінансової звітності»

		КОДИ			
	Дата (рік, місяць, число)	<table border="1"><tr><td></td><td></td><td>01</td></tr></table>			01
		01			
Підприємство ТОВ "МІРОПЛАСТ"	за ЄДРПОУ	34230288			
Територія м.Дніпро	за КОАТУУ				
Організаційно-правова форма господарювання ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ	за КОПФГ				
Вид економічної діяльності 22.21 Виробництво пластмасових листів, камер для шин и профілів	за КВЕД				

Середня кількість працівників¹ _____

Адреса, телефон 49083, Дніпропетровська обл., місто Дніпро, Амур-Нижньодніпровський район, ВУЛИЦЯ СОБИНОВА, будинок 1

Одиниця виміру: тис.грн. без десяткового знака (окрім розділу IV Звіту про фінансові результати (Звіту про сукупний дохід) (форма N 2), грошові показники якого наводяться в гривнях з копійками)

Складено (зробити позначку «v» у відповідній клітинці):

за положеннями (стандартами) бухгалтерського обліку

за міжнародними стандартами фінансової звітності

БАЛАНС
(Звіт про фінансовий стан)
на 31 грудня 2020 р.

Форма № 1	Код за ДКУД		1801001
Актив	Код рядка	На початок звітного періоду	На кінець звітного періоду
1	2	3	4
I. Необоротні активи			
Нематеріальні активи	1000		
первісна вартість	1001	1 590,2	1 590,2
накопичена амортизація	1002	(338,4)	(348,8)
Незавершені капітальні інвестиції	1005		14 789,9
Основні засоби	1010	141 863,5	170 098,5
первісна вартість	1011	184 054,2	203 864,1
знос	1012	(42 190,7)	(33 765,6)
Інвестиційна нерухомість	1015		
Довгострокові біологічні активи	1020		
Довгострокові фінансові інвестиції: які обліковуються за методом участі в капіталі інших підприємств	1030		
інші фінансові інвестиції	1035		
Довгострокова дебіторська заборгованість	1040	17 318,5	
Відстрочені податкові активи	1045		
Інші необоротні активи	1090		
Усього за розділом I	1095	160 433,8	186 129,8
II. Оборотні активи			
Запаси	1100	71 723,1	82 857,4
Поточні біологічні активи	1110		
Дебіторська заборгованість за продукцію, товари, роботи, послуги	1125		
Дебіторська заборгованість за розрахунками: за виданими авансами	1130	27 006,1	27 006,1
з бюджетом	1135	16 305,8	
у тому числі з податку на прибуток	1136		
Інша поточна дебіторська заборгованість	1155	19 533,1	26 504,5
Поточні фінансові інвестиції	1160	14 058,7	12 834,6
Гроші та їх еквіваленти	1165	12 944,0	15 999,9
Витрати майбутніх періодів	1170		
Інші оборотні активи	1190		
Усього за розділом II	1195	189 649,2	214 641,7
III. Необоротні активи, утримувані для продажу, та групи вибуття	1200	1 775,2	2 113,7
Баланс	1300	351 858,2	402 885,2

Пасив	Код рядка	На початок звітнього періоду	На кінець звітнього періоду
1	2	3	4
I. Власний капітал			
Зареєстрований (пайовий) капітал	1400	37 008,2	37 008,2
Капітал у дооцінках	1405		
Додатковий капітал	1410	15 979,3	15 979,3
Резервний капітал	1415		
Нерозподілений прибуток (непокритий збиток)	1420	140 719,1	163 336,2
Неоплачений капітал	1425	()	()
Вилучений капітал	1430	()	(7 294,7)
Усього за розділом I	1495	193 706,6	209 029,0
II. Довгострокові зобов'язання і забезпечення			
Відстрочені податкові зобов'язання	1500		
Довгострокові кредити банків	1510	26 881,0	
Інші довгострокові зобов'язання	1515		
Довгострокові забезпечення	1520		
Цільове фінансування	1525		
Усього за розділом II	1595	26 881,0	
III. Поточні зобов'язання і забезпечення			
Короткострокові кредити банків	1600	31 069,1	
Поточна кредиторська заборгованість за: довгостроковими зобов'язаннями	1610		
товари, роботи, послуги	1615	83 633,4	154 056,4
розрахунками з бюджетом	1620		5 578,3
у тому числі з податку на прибуток	1621		7 263,8
розрахунками зі страхування	1625		12 305,6
розрахунками з оплати праці	1630	16 568,1	14 652,1
Поточні забезпечення	1660		
Доходи майбутніх періодів	1665		
Інші поточні зобов'язання	1690		
Усього за розділом III	1695	131 270,6	193 856,2
IV. Зобов'язання, пов'язані з необоротними активами, утримуваними для продажу, та групами вибуття	1700		
Баланс	1900	351 858,2	402 885,2

Керівник

Головний бухгалтер

¹ Визначається в порядку, встановленому центральним органом виконавчої влади, що реалізує державну політику у сфері статистики.

Дата (рік, місяць, число)

Підприємство ТОВ «МІРОПЛАСТ»

(найменування)

за ЄДРПОУ

Звіт про фінансові результати (Звіт про сукупний дохід)

за _____ 2020 р.

Форма № 2 Код за ДКУД

1801003

КОДИ

01

I. Фінансові результати

Стаття	Код рядка	За звітний період	За аналогічний період попереднього року
1	2	3	4
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000	930 463,7	815 308,0
Собівартість реалізованої продукції (товарів, робіт, послуг)	2050	(830 385,7)	(716 422,8)
Валовий: прибуток	2090	100 078,0	98 885,2
збиток	2095	()	()
Інші операційні доходи	2120	53 673,2	53 961,9
Адміністративні витрати	2130	(25 732,3)	(28 714,4)
Витрати на збут	2150	(39 749,2)	(25 638,2)
Інші операційні витрати	2180	(73 808,3)	(89 394,7)
Фінансовий результат від операційної діяльності: прибуток	2190	14 461,4	9 099,8
збиток	2195	()	()
Дохід від участі в капіталі	2200	13 754,9	10 459,4
Інші фінансові доходи	2220	6 574,4	6 879,2
Інші доходи	2240	7 393,3	6 570,8
Фінансові витрати	2250	(7 328,5)	(6 476,9)
Втрати від участі в капіталі	2255	()	()
Інші витрати	2270	(5 842,3)	(6 844,7)
Фінансовий результат до оподаткування: прибуток	2290	29 013,2	19 687,6
збиток	2295	()	()
Витрати (дохід) з податку на прибуток	2300	(6 396,1)	(4 183,3)
Прибуток (збиток) від припиненої діяльності після оподаткування	2305		
Чистий фінансовий результат: прибуток	2350	22 617,1	15 504,3
збиток	2355	()	()

II. СУКУПНИЙ ДОХІД

Стаття	Код рядка	За звітний період	За аналогічний період попереднього року
Дооцінка (уцінка) необоротних активів	2400		
Дооцінка (уцінка) фінансових інструментів	2405		
Накопичені курсові різниці	2410		
Частка іншого сукупного доходу асоційованих та спільних підприємств	2415		
Інший сукупний дохід	2445		
Інший сукупний дохід до оподаткування	2450		
Податок на прибуток, пов'язаний з іншим сукупним доходом	2455		
Інший сукупний дохід після оподаткування	2460		
Сукупний дохід (сума рядків 2350, 2355 та 2460)	2465	22 617,1	15 504,3

III. ЕЛЕМЕНТИ ОПЕРАЦІЙНИХ ВИТРАТ

Матеріальні затрати	2500	432389,50	399073,80
Витрати на оплату праці	2505	64117,8	61380,2
Відрахування на соціальні заходи	2510	11038,30	9876,20
Амортизація	2515	18046,50	11976,40
Інші операційні витрати	2520	13670,00	15035,00
Разом	2550	539262,1	497341,6

Сертифікати якості продукції ТОВ «МІРОПЛАСТ»

 МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ ДЕРЖАВНА СИСТЕМА СЕРТИФІКАЦІЇ УкрСЕПРО		Серія ВГ
СЕРТИФІКАТ ВІДПОВІДНОСТІ UA1.196.0026572-15		
Зареєстровано в Реєстрі за № _____		
Зареєстрований в Реєстрі		
Термін дії з	20 травня 2015	до 19 травня 2017
Срок дієвості с		
Продукція	Профілі полівінілхлоридні для віконних та дверних конструкцій	
Продукція	торгових марок: 'WDS', 'TRIO', 'GALAXY', 'Olimpia'	
		код УКТ ЗЕД, ТН ЗЕД 22.21.10 код ДІПТ, ОКП
Відповідає вимогам	ДСТУ Б В.2.7-130:2007 п.п. 5.2.3 - 5.2.5, 5.3.1 (табл. 3, п.п. 5, 7), 5.3.7	
Споживається переважно		
Виробник продукції	ТОВ 'МІРОПЛАСТ', м. Дніпропетровськ, вул. Собінова, 1, код ЄДРПОУ 34230288, адреса виробництва: 49051, Дніпропетровськ, вул. Курсантська, 10	
Сертифікат видано	ТОВ 'МІРОПЛАСТ', 49083, м. Дніпропетровськ, вул. Собінова, 1, код ЄДРПОУ 34230288	
Додаткова інформація	Профілі полівінілхлоридні для віконних та дверних конструкцій торгових марок: 'WDS', 'TRIO', 'GALAXY', 'Olimpia', які виготовляються серійно з 20.05.2015 р. до 19.05.2017р., з урахуванням гарантійного терміну зберігання, технічний нагляд один раз на рік	
Сертифікат видано органом з сертифікації	ТОВ 'ВЕС 'УКРЕКСПЕРТИЗА', м. Запоріжжя, вул. Північне шосе, 3, свідоцтво про призначення № UA.P.196 від 10.02.2015 р./ свідоцтво про уповноваження № UA.PN.196 від 10.02.2015р. т. (061)212-31-48, ves.ukrexpertiza@gmail.com, www.ves.in.ua	
На підставі	Протоколу сертифікаційних випробувань № Т91/05-15 від 20.05.2015, виданого ВЛ ТОВ ВСЦ	
На основі:	'Підентест', м. Дніпропетровськ, 49064, пр-т. Капініна, 50, атестат акредитації № 2Н485 від 25.10.2013 р. до 24.10.2018 р. Акт обстеження № 196-125/04-15 від 20.05.20 15р.	
Керівник органу з сертифікації	К.О. Єрмоленко	
Розробник органу з сертифікації	ініціали, прізвище	
М.П.	Чисельність сертифіката відповідності можна перевірити в Реєстрі системи УкрСЕПРО за код. (044) 517-35-76	


НАЦІОНАЛЬНИЙ ОРГАН УКРАЇНИ З СЕРТИФІКАЦІЇ

Система сертифікації УкрСЕПРО

СЕРТИФІКАТ НА СИСТЕМУ УПРАВЛІННЯ ЯКІСТЮ

Зареєстрований у Реєстрі
Системи сертифікації УкрСЕПРО
«24» січня 2011 р.
№ UA.2.037.05721-11
Дійсний до «24» січня 2016р.

ЦИМ СЕРТИФІКАТОМ ПОСВІДЧУЄТЬСЯ, ЩО СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ СТОСОВНО:
виробництва профілів полівінілхлоридних для огорожувальних будівельних конструкцій
(код ДКПП 25.21.10)

(назва продукції, вид, марка, код ДКПП- і/або код ТН ЗЕД)

які виготовляє Товариство з обмеженою відповідальністю «МІРОПЛАСТ»
(назва підприємства-виробника)
Юридична адреса: 49083, м. Дніпропетровськ, вул. Собінова, 1
Виробництво: 49051, м. Дніпропетровськ, вул. Курсантська, 10
код ЄДРПОУ 34230288
(адреса, код ЄДРПОУ)

згідно з нормативними документами, чинними в Україні

ВІДПОВІДАЄ ВИМОГАМ ДСТУ ISO 9001:2009 «Системи управління якістю. Вимоги»
(позначення стандарту на систему управління якістю)

Контроль відповідності сертифікованої системи управління якістю вимогам зазначеного стандарту здійснюється шляхом технічного нагляду, періодичність і процедури якого регламентуються програмою.

СЕРТИФІКАТ ВИДАНИЙ Органом з сертифікації систем управління
державного підприємства «Дніпропетровський регіональний державний
науково-технічний центр стандартизації, метрології та сертифікації»
(ДП «Дніпростандартметрологія»),
(назва органу з сертифікації, що видав сертифікат,
49044, м. Дніпропетровськ, вул. Барикадна, 23, т. (0562) 39-86-09,
його адреса,
свідоцтво про призначення № UA.MQ.037 від 24 квітня 2008 р.
номер атестата акредитації і дата реєстрації)

НА ПІДСТАВІ РЕЗУЛЬТАТІВ ПЕРЕВІРКИ ТА ОЦІНКИ СИСТЕМИ УПРАВЛІННЯ ЯКІСТЮ



В.М. Сервініна
керівниця органу з сертифікації



(підпис)

В.М.Чайка
(ініціали, прізвище)

СЕРТИФІКАТ

MIROPLAST

ISO 9001:2008

DEKRA Certification Sp. z o.o. засвідчує, що в організації

**Товариство з обмеженою відповідальністю
«МІРОПЛАСТ»**

Область сертифікації:

Виробництво і продаж профілів полівінілхлоридних

Адреса:

вул. Курсантська, 10, м. Дніпропетровськ, 49051, Україна

впроваджена і застосовується система менеджменту якості відповідно до вимог вищезазначеного стандарту. Сертифікат виданий на підставі аудиторського звіту № W-A 617415/A12/P/9001.

Даний сертифікат дійсний з 2015-04-11 по 2018-04-10

Реєстраційний № сертифіката:
320412036/1



DEKRA Certification Sp. z o.o.
Wrocław, 2015-04-09



При порушенні умов договору -> сертифікацію сертифікат одразу втрачає свою силу

DEKRA Certification GmbH • Handwerkstraße 15 • D-70565 Stuttgart • www.dekra-certification.com

Сторінка 1 з 1