Міністерство освіти і науки України Дніпровський державний аграрно-економічний університет
Факультет обліку і фінансів
Кафедра обліку, оподаткування та управління фінансово-економічною безпекою

ДОПУСТИТИ ДО ЗАХИСТУ
В ЕКЗАМЕНАЦІЙНІЙ КОМІСІЇ:

В.о. завідувача кафедри,
к.е.н., доцент
_____Ольга ГУБАРИК
«____» _____ 20___ р.

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«Удосконалення процесу захисту фінансово-економічної безпеки підприємства від ризиків шахрайства»**
Освітньо-професійна програма «Управління фінансово-економічною безпекою»
Спеціальність 073 «Менеджмент»
Рівень вищої освіти: другий (магістерський)

Здобувач
групи МгУФЕБз-23 Віталій ВІТЕР

Науковий керівник,
к.е.н., доцент Ольга ОДНОШЕВНА
науковий ступінь, посада

Дніпро – 2024

ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ АГРАРНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Факультет: Обліку і фінансів
Кафедра: Обліку, оподаткування та управління фінансово-економічною безпекою
Освітньо-професійна програма: «Управління фінансово-економічною безпекою»
Спеціальність: 073 «Менеджмент»
Рівень вищої освіти: другий (магістр)

З А Т В Е Р Д Ж У Ю
В.о. завідувача кафедри _____ Ольга ГУБАРИК
«_____»_____ 202__р.

З А В Д А Н Н Я

ВІТРУ ВІТАЛІЮ АНДРІЙОВИЧУ

(прізвище, ім'я, по батькові)

1. Тема роботи: **Удосконалення процесу захисту фінансово-економічної безпеки підприємства від ризиків шахрайства**
2.
3. Науковий керівник: Одношевна Ольга Олександрівна, к.е.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по ДДАЕУ від « 09 » жовтня 2024 року № 3363
4. Термін подання здобувачем роботи: 10 грудня 2024 р.
5. Вихідні дані до роботи: Закони України, Постанову Кабінету Міністрів України**,** методичні рекомендації і інші нормативні документи, навчальні посібники, фахові статті, дані бухгалтерського обліку і фінансової звітності ТОВ Агрофірма «Славутич»
6. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Теоретичне дослідження сутності важливих даних та комерційної таємниці підприємства. Проведення аналізу фінансово-економічної безпеки та захисту комерційної таємниці на ТОВ Агрофірма «Славутич». Удосконалення захисту вразливих даних від несанкціонованого доступу на ТОВ Агрофірма «Славутич». Висновки. Список використаних джерел.
7. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Визначення поняття комерційної таємниці та важливих даних Комерційна таємниця у господарській діяльності, типи та форми. Планування, оцінювання та аналіз захисту важливих даних. Досвід захисту комерційної таємниці та важливих даних з вітчизняних та зарубіжних джерел. Характеристика фінансово економічної діяльності ТОВ Агрофірма «Славутич Дослідження та оцінка роботи відділу економічної безпеки на підприємстві ТОВ Агрофірма «Славутич». Дослідження поточного захисту комерційної таємниці та вразливих даних у ТОВ Агрофірма «Славутич». Значення інформаційної безпеки в умовах сучасного бізнес-середовища. Основні загрози та виклики для інформаційної безпеки підприємства. Розробка концепції вдосконалення інформаційної безпеки: система протидії фішинговим атакам із застосуванням сучасних методів шифрування.

8. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____Березень 2024_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Теоретичне дослідження сутності важливих даних та комерційної таємниці підприємства	Березень 2024	
2.	Проведення аналізу фінансово-економічної безпеки та захисту комерційної таємниці на ТОВ Агрофірма «Славутич»	Квітень 2024	
3.	Удосконалення захисту вразливих даних від несанкціонованого доступу на ТОВ Агрофірма «Славутич»	Травень 2024	
4.	Висновки і пропозиції	Вересень 2024	
5.	Оформлення роботи	Жовтень 2024	

Здобувач_____ Віталій ВІТЕР
(підпис) (прізвище та ініціали)

Науковий керівник_____ Ольга ОДНОШЕВНА
(підпис) (прізвище та ініціали)

ЗМІСТ

РЕФЕРАТ

Тема: «Удосконалення процесу захисту фінансово-економічної безпеки підприємства від ризиків шахрайства»

Кваліфікаційна робота містить: 81 с., 19 рис., 3 табл., 58 літературних джерел, 1 додаток.

Об'єктом дослідження є процес забезпечення фінансово-економічної безпеки підприємства.

Предмет дослідження – організаційно-правові та технологічні заходи із захисту фінансово-економічної безпеки підприємства від ризиків шахрайства.

Метою дослідження є розробка шляхів удосконалення процесу захисту фінансово-економічної безпеки підприємства з акцентом на мінімізацію ризиків шахрайства.

Методи дослідження: У роботі використано загальнонаукові та спеціальні методи дослідження, зокрема діалектичний метод для аналізу економічних понять, методи синтезу, порівняння та систематизації для дослідження системи захисту інформації. Для оцінки фінансових показників підприємства застосовано методи статистичного аналізу.

У дослідженні узагальнено теоретичні аспекти формування системи фінансово-економічної безпеки підприємства, що спрямовані на протидію шахрайським діям. Проаналізовано основні загрози, пов'язані з шахрайством у фінансово-економічній діяльності, та визначено слабкі місця у системі захисту комерційної інформації.

Робота включає аналіз фінансово-економічної діяльності ТОВ Агрофірма «Славутич». Проведено оцінку технічного стану основних засобів, рівня інформаційної безпеки та ефективності використання кадрових ресурсів. У першому розділі приділено увагу загрозам, які виникають унаслідок людського фактору, кібератак та недостатнього оновлення технічної інфраструктури. У третьому розділі запропоновано заходи для покращення захисту фінансово-економічної безпеки підприємства: впровадження гібридних методів шифрування для захисту комерційної інформації, розробка системи моніторингу підозрілих операцій для запобігання шахрайству, модернізація технічних засобів та навчання персоналу основам кібербезпеки.

Запропоновано модель організаційного забезпечення економічної безпеки, яка поєднує технічні, правові та управлінські заходи.

Результати дослідження впроваджено в практичну діяльність ТОВ Агрофірма «Славутич».

КЛЮЧОВІ СЛОВА

ФІНАНСОВО-ЕКОНОМІЧНА БЕЗПЕКА, ШАХРАЙСТВО, ЗАХИСТ ІНФОРМАЦІЇ, МОНІТОРИНГ ЗАГРОЗ, РИЗИК-МЕНЕДЖМЕНТ, УПРАВЛІННЯ БЕЗПЕКОЮ.

ABSTRACT

Topic: "Improving the Process of Protecting the Financial and Economic Security of an Enterprise from Fraud Risks"

The qualification work consists of: 81 pages, 19 figures, 3 tables, and 58 sources,1 application.

The object of the research is the process of ensuring the financial and economic security of an enterprise.

The subject of the research is organizational, legal, and technological measures for protecting the financial and economic security of an enterprise from fraud risks.

The aim of the research is to develop ways to improve the process of protecting the financial and economic security of an enterprise, focusing on minimizing fraud risks.

Research methods: The work employs general scientific and specialized research methods, including the dialectical method for analyzing economic concepts, methods of synthesis, comparison, and systematization to study the information protection system. For evaluating the financial indicators of the enterprise, statistical analysis methods are used.

Content of the Work

The study summarizes the theoretical aspects of forming a financial and economic security system for enterprises aimed at countering fraudulent activities. The main threats related to fraud in financial and economic activities are analysed, and the weaknesses in the commercial information protection system are identified.

The work includes an analysis of the financial and economic activities of LLC Agrofirma «Slavutych». An evaluation of the technical condition of the main assets, the level of information security, and the effectiveness of human resource utilization is carried out. Attention is given to the threats arising from the human factor, cyberattacks, and insufficient updating of the technical infrastructure.

Measures to improve the protection of financial and economic security are proposed, including the implementation of hybrid encryption methods to protect commercial information, the development of a suspicious transaction monitoring system to prevent fraud, the modernization of technical means, and training staff in cybersecurity basics.

A model for organizational support of economic security is proposed, combining technical, legal, and management measures.

The research results have been implemented in the practical activities of LLC Agrofirma «Slavutych».

KEYWORDS

FINANCIAL AND ECONOMIC SECURITY, FRAUD, INFORMATION PROTECTION, THREAT MONITORING, RISK MANAGEMENT, SECURITY MANAGEMENT.

ВСТУП

В умовах сьогодення все більшою та значною стає увага щодо захисту важливих даних та елементів комерційної таємниці. Насамперед це зумовлюється тим, що різко збільшується обмін інформацією між людьми через швидкість, зручність, та якість обміну даними. Але й через нововведення з'являються нові шляхи для несанкціонованого доступу до важливих даних якими зловмисники бажають заволодіти заради особистої вигоди. Дослідження присвячується аналізу які дані необхідно захистити, які для цього існують правові врегулювання, якими методами користуються передові компанії та розробка власного оригінального рішення поставленої задачі.

Вивчення сучасного стану законодавства та правозастосовної практики в Україні вказує на необхідність удосконалення механізмів захисту комерційної інформації. Зокрема, існуючі прогалини у нормативно-правовій базі та недосконале застосування чинних положень можуть призвести до серйозних фінансових і репутаційних втрат для підприємств. Отже, важливим завданням є проведення досліджень, що дозволять виявити проблемні питання у сфері захисту комерційної таємниці та розробити ефективні підходи для їх вирішення.

Метою цієї кваліфікаційної роботи є глибоке дослідження та аналіз організаційно-правових механізмів захисту комерційної таємниці та вразливих даних. У роботі для цієї мети поставлені такі завдання:

1. Розкрити поняття та правове регулювання комерційної таємниці та її значення для фінансово-економічної безпеки компаній.
2. Проаналізувати організаційні заходи та практичних аспектів, спрямовані на збереження конфіденційності інформації у компаніях.
3. Розробити нові наукові підходи для покращення захисту комерційної таємниці та вдосконалити існуючі.

Предметом виконання кваліфікаційної роботи є дослідження процесу функціонування системи економічної безпеки в розрізі захисту комерційної таємниці та важливих даних господарюючого суб’єкта.

Об’єктом дослідження виступає безпосередній захист комерційної таємниці та вразливих даних у суб’єктів господарської діяльності, а також організаційно-правове забезпечення цього процесу.

Для реалізації поставлених завдань були застосовані такі методи дослідження: Аналіз наукової літератури, присвяченої комерційній таємниці та фінансово-економічній безпеці. Дослідження законодавчих актів України з питань захисту комерційної таємниці. Аналіз та узагальнення практичного досвіду застосування організаційно-правових заходів для захисту комерційної інформації. Емпіричні методи, зокрема анкетування та інтерв'ю з експертами у відповідній галузі.

Наукова новизна цієї роботи полягає у розробці та вдосконаленні методів управління комерційною таємницею, які включають впровадження вдосконаленої технології шифрування даних. Основні результати, які виражені у наступній наукові новизні:

вперше:

- запропоноване програмне забезпечення яке буде реагувати на фішингові повідомлення які надходять до компанії, та завчасно інформувати про це виконуючу особу. Такий підхід зменшить час на навчання персоналу, зменшить вплив людського фактору на захист вразливих даних, підвищить конкурентоспроможність підприємства та довіру клієнтів до нього.

удосконалено:

- Підхід до визначення та аналізу вразливих даних, поділ їх на класи та розподіл за авторитетністю. Удосконалено підхід до визначення комерційної таємниці на підприємстві, підвищені алгоритми реагування на ознаки шахрайських дій. Удосконалено визначення стратегічного напрямку діяльності підприємства за розрахунком його фінансових показників.

набуло подальшого розвитку:

- Розвиток програмного забезпечення на мові програмування Python для підвищення фінансово-економічних показників безпеки на підприємстві. Трактування поняття комерційної таємниці, розподіл за класифікаціями вразливих даних та комерційної таємниці.

Особистий внесок відображається у визначенні підходів щодо роботи яка стосується фінансово-економічної безпеки, та висвітленню необхідних етапів управління для підвищення показника захищеності важливих даних на ТОВ Агрофірма «Славутич».

Апробація результатів дослідження. Основні напрямки кваліфікаційної роботи обговорювалися на наукових конференціях з робіт кафедри обліку, оподаткування та управління фінансово-економічною безпекою, а також у міжвузівському науково-практичному семінарі: «Економіка та інформаційні технології: управління та виклики сьогодення» 18 квітня 2024 року. Також відзначено нагородою переможця І туру Всеукраїнського конкурсу студентських наукових робіт галузі знань 073 «Менеджмент» ОПП «Управління фінансово-економічною безпекою у 2023-2024 навчальному році.

Публікації. За отриманими результатами по темі роботи опубліковано наукова праця у міжвузівському семінарі наукових робіт у приватний вищий навчальний заклад «Буковинський університет», одна фахова стаття у науковому журналі категорії Б «Бізнес-Інформ» №9, 2024, дві тези у матеріалах конференції збірника наукових тез ДДАЕУ.

РОЗДІЛ 1. ТЕОРЕТИЧНЕ ДОСЛІДЖЕННЯ СУТНОСТІ ВАЖЛИВИХ ДАНИХ ТА КОМЕРЦІЙНОЇ ТАЄМНИЦІ ПІДПРИЄМСТВА

1.1 Визначення поняття комерційної таємниці та важливих даних

Захист комерційної таємниці (*далі КТ*) є ключовим елементом безпеки підприємств та суб'єктів господарської діяльності який привертає значну увагу як у науковій, так і у практичній сфері. Її визначення та розуміння варіюється залежно від контексту і специфіки господарської діяльності кожного підприємства. У сучасній науковій літературі існує кілька підходів до трактування цього поняття, які відображають різні підходи захисту та використання комерційної інформації.

Відповідно до цивільного кодексу України поняття комерційної таємниці визначено наступним чином: «Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою» [42]. Також нормативний акт висвітлює КТ: « Не є легкодоступною для осіб, які звичайно мають справу з видом інформації до якого вона належить» [42]. Продовжуючи визначення: «Має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію» [42].

КТ може бути представлена у різноманітних формах, таких як технічні процеси, методи виробництва, формули, дані про продажі та маркетинг, база клієнтів та інша інформація, важлива для діяльності підприємства. Вся ця інформація сприяє збереженню конкурентних переваг на ринку і дозволяє компанії утримувати свою унікальну позицію серед конкурентів. У будь якій підприємницькій діяльності необхідно приділяти увагу захисту конфіденційної інформації, оскільки вона може визначати їхню

конкурентоспроможність. У сучасному середовищі та різноманітним способам ведення підприємництва, де обмін інформацією став швидким і легкодоступним, забезпечення конфіденційності стає критично важливим завданням для компаній незалежно від їхніх розмірів чи форми власності. Серед необхідної для захисту інформації також є стратегічні плани, ринкові стратегії, інноваційні проєкти, які формують основу конкурентної сили підприємства.

Хлевицька Т.Б. та Гусєва Ю.А. пишуть: «Оцінка рівня фінансово-економічної безпеки підприємства може здійснюватися в різних тимчасових аспектах – поточному та прогнозному» [44]. Продовжуючи думку стверджують: «Поточна оцінка є найбільш точною та носить констатуючий характер. Прогнозна оцінка носить імовірнісний характер, що пов’язане з прогнозуванням розміру необхідних показників» [44]. Інформаційна безпека передбачає системний підхід до управління ризиками, а також забезпечення цілісності та захисту інформаційних ресурсів. З цієї точки зору, захист комерційної таємниці є не просто обмеженням доступу до окремих даних, а й стає стратегічним інструментом управління бізнес-процесами. Одним із сучасних підходів у сфері інформаційного захисту є концепція «захисту через ризик», яка полягає в ідентифікації ризиків, оцінці їхнього потенційного впливу та управлінні ними [54]. Використовуючи такий підхід, з’являється краща можливість відділу управлінням фінансово-економічної безпеки аналізувати чутливу інформації, визначати найбільш вразливі дані та проставивши пріоритети, краще на них фокусуватися. Такій підхід дозволяє оптимізувати використання ресурсів та знизити витрати на захист конфіденційних даних.

1.2 Комерційна таємниця у господарській діяльності, типи та форми. Планування, оцінювання та аналіз захисту важливих даних

При дослідженні типів та форм комерційної таємниці та вразливих даних слід враховувати фактори та характеристики, які залежать від специфіки та умов діяльності конкретного господарського суб’єкта. Це означає, що кожна організація має власні унікальні види комерційної інформації, які важливо вивчити для побудови ефективної системи захисту.

Кравченко М.В. пише: «Механізм управління забезпеченням фінансової безпеки суб'єктів господарювання потребує множини взаємопов'язаних дій, що об’єднуються в системний підхід до підтримки фінансової безпеки підприємств»[22]. Згідно з дослідженнями, комерційна таємниця може класифікуватися залежно від її сутності та призначення. Одним із видів такої інформації є технологічні розробки, що включають винаходи, виробничі процеси й інші інновації в технічній сфері. Іншим видом є дані, що стосуються стратегічного планування, маркетингових стратегій і досліджень ринку [38]. Слід звернути увагу, що багато видів комерційної інформації можуть перетинатися, що ускладнює класифікацію та підвищує важливість індивідуального підходу до захисту. Також можна класифікувати чутливу інформацію за об’єктивними характеристиками, зокрема на технічну, фінансову, інформаційну та інші форми, також варто відмітити що: «Зміцнення економічної безпеки підприємства передбачає реалізацію заходів, які б забезпечили досягнення максимально можливого її рівня» [22]. Для прикладу, технічна таємниця охоплює виробничі процеси і технологічні інновації, тоді як фінансова стосується даних про витрати, структуру цін тощо [36].

Касьянова та Кравчук наголошують: «Захист же від внутрішніх загроз набагато складніший та вимагає великих зусиль, а також витрат» [15]. Продовжуючи думку вони стверджують: «Він полягає у забезпеченні безпеки

самих додатків та грамотному адмініструванні, яке означає, що співробітників компанії мають чіткі привілеї щодо доступу до інформаційних ресурсів підприємства» [15].

Проведення такого аналізу процесів дозволяє визначити, які складові комерційної таємниці є критичними для стабільного розвитку компанії. Одним із важливих елементів класифікації комерційної таємниці є рівень її захисту. Кожен вид інформації потребує особливого підходу до захисту, що визначається його цінністю та потенційними ризиками витоку. Проаналізувавши літературні джерела можна стверджувати що технічні винаходи найчастіше захищаються патентами, що забезпечує юридичний захист і ексклюзивне право на їх використання. Однак для інших видів даних, таких як стратегії чи маркетингові плани, які не підлягають патентуванню, потрібно застосовувати угоди про конфіденційність або механізми захисту інтелектуальної власності [30].

Також з досліджень пишуть що: «Базовим елементом інформаційно-аналітичного забезпечення управління фінансово-економічною безпекою є облікова інформація» [25]. Звертаючи увагу на сучасний розвиток ведення бізнесу, технологіями управління та методами обміну інформації разом отриманими новими перевагами з’являються також нові вразливі місця, якими можуть скористатися зловмисники. У зв’язку з цим з’являється потреба в постійному удосконаленні методів захисту чутливої інформації та організаційних заходів безпеки.

Васільєва Л.М. та Іжболдін М.М. вважають: «Забезпечення інформаційної безпеки підприємницької діяльності - це процес застосування різних заходів, політик, технологій та практик з метою забезпечення конфіденційності» [14]. Для забезпечення захисту комерційної таємниці необхідно використовувати комплексний підхід до планування ефективних стратегій. Починати слід з проведення аналізу та оцінювання загроз що дасть змогу виявити можливі ризики, визначити вразливі місця і оцінити

ймовірність витоку або несанкціонованого використання цінної інформації. До планування заходів захисту слід віднести розробку та впровадження стратегій, процедур і політик, що знижують ці ризики і забезпечують надійний захист комерційних даних.

Для аналізу і оцінювання захисних механізмів передбачене ретельне вивчення всіх процесів та методів, що стосуються захисту інформації яка має найбільш значний та критичний вплив на функціонування підприємства. У ході аналізу враховуються як внутрішні, так і зовнішні загрози, здатні порушити конфіденційність інформаційних ресурсів компанії.

Першим кроком в аналізі є визначення можливих джерел загроз, які можуть бути як зовнішніми (кібератаки, дії хакерів), так і внутрішніми (недбалість співробітників, шахрайські дії або зловживання даними) [28]. Після цього оцінюється можливий вплив цих загроз на бізнес-процеси компанії. Після цього виконується ідентифікація слабких місць у системі захисту, які зловмисники можуть використати для доступу до конфіденційної інформації [24]. Після виявлення цих вразливих точок, компанія буде мати кращу позицію в розумінні вразливої інформації що дасть змогу обрати оптимальні методи для підвищення рівня захищеності.

До типових вразливостей збереження комерційної інформації слід віднести наступні. Типові порушення представлені на рисунку 1.1.

Одним з основних чинників що послаблює захист компанії у цифровому середовищі є несвоєчасне оновлення програмного забезпечення. Програми, операційні системи та додатки, містять у собі певні вразливості, які хакери можуть використати для отримання несанкціонованого доступу. Також проблемою є використання слабких паролів або недостатньо ефективні методи аутентифікації. Якщо компанія не використовує надійні паролі чи додаткові рівні аутентифікації, система стає більш вразливою до атак.

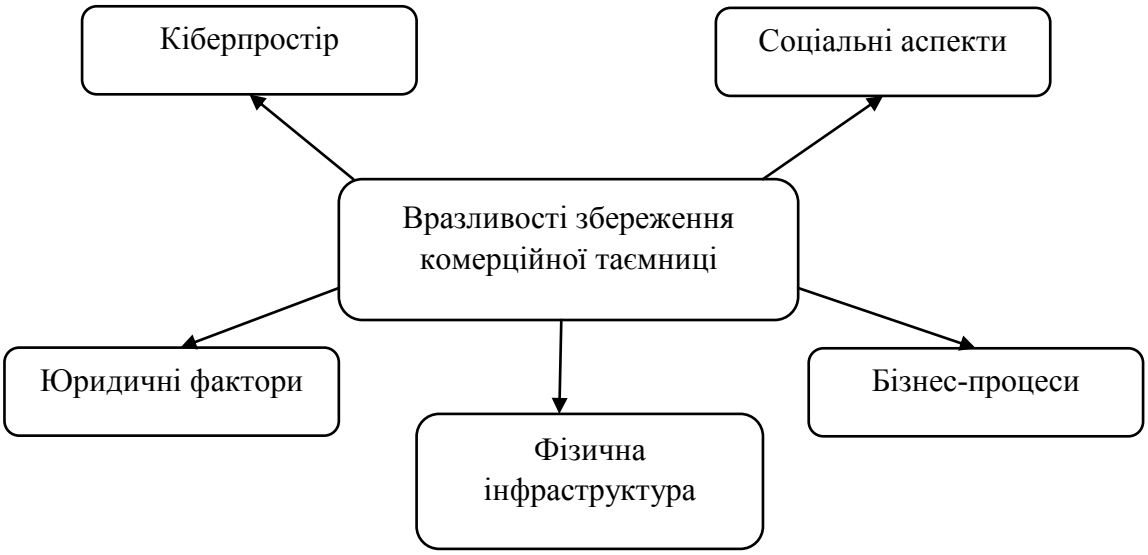

Рис. 1.1. Вразливості збереження КТ

Недостатній захист мережі – ще один критичний елемент. Відсутність фаєрволів, низький рівень сегментації мережі та неправильне налаштування мережевих пристроїв, такі недоліки підвищують вразливість системи до зовнішніх атак. Відсутність оновлень і патчів збільшує ризики в захисті вразливих даних так як потенційні вразливості залишаються невиправленими.

Також Васльєва Л.М. та Іжболдін М.М. пишуть: «Визначено механізми та підходи до забезпечення інформаційної безпеки підприємницької діяльності як складової інформаційної безпеки держави: законодавча база; стандарти і рекомендації» [14]. Продовжуючи думку вони відзначають що до цього відноситься: «спільні проекти та обмін інформацією; навчання і освіта; створення інфраструктури безпеки; моніторинг та відгук на інциденти; співробітництво з міжнародними організаціями» [14]. Через людський фактор підприємницька діяльність також може мати підвищені ризики до безпечної діяльності компанії. Недостатня обізнаність персоналу щодо кібербезпеки може призвести до ряду помилок, як неправильне поводження з електронною поштою чи створення слабких паролів. При недотриманні визначених компанією правил роботи та послідовності дій зловмисники

матимуть більше шансів в успішному використанні фішингових атаки, щоб отримати доступ до конфіденційної інформації або фінансових ресурсів. Співробітник може ненавмисно відкрити підозріле повідомлення або перейти за фішинговим посиланням, надаючи шахраям можливість заволодіти даними для входу в систему.

Маслак Ольга та Ярослав Яковенко пишуть: «Підприємства, які орієнтуються на майбутнє (інтерактивна позиція), мають два варіанти: керувати змінами або передбачати їх»[29]. Також вони відмічають «Активно впливаючи на зовнішнє середовище або готуючись до майбутніх змін, підприємства можуть краще адаптуватися до кіберзагроз і захистити свої активи» [29]. Слабкі паролі, такі як використання дати народження або популярних слів, полегшують процес злому, що особливо небезпечно в середовищах, де проводяться фінансові операції або обробляються персональні дані клієнтів. Для підвищення рівня безпеки є регулярне навчання співробітників з питань кібербезпеки та впровадження політик щодо управління паролями та безпечної роботи з електронною поштою.

Фізичні вразливості охоплюють недоліки в інфраструктурі компанії, що можуть створити точки доступу для потенційних загроз. Це можуть бути погано захищені входи, двері, вікна або ворота, де відсутність контролю дозволяє неавторизованим особам потрапити на територію компанії або до обладнання. Крім того, недостатня якість відеоспостереження та інші системи захисту можуть створювати небезпеку для фізичної безпеки приміщень або майна підприємства.

Захист КТ передбачає ретельне планування ефективних заходів і стратегій безпеки. Він включає аналіз і оцінку потенційних загроз для виявлення слабких місць, а також розробку процедур для уникнення витоків або зловживань конфіденційною інформацією. Планування таких заходів передбачає впровадження політик, що зменшують ризики та забезпечують належний захист важливих даних.

Аналіз та оцінка захисту КТ – наступний важливий етап створення безпекової стратегії для будь-якого підприємства. Цей процес охоплює комплексне дослідження всіх аспектів, які мають значення для захисту інформації компанії, враховуючи як зовнішні, так і внутрішні загрози, що можуть поставити під загрозу конфіденційність даних.

Першим етапом є визначення всіх можливих джерел загроз. Вони можуть бути зовнішніми, як кібератаки, або внутрішніми, людські помилки, шахрайство чи неналежне використання даних [20]. Після цього оцінюється потенційний вплив таких загроз на діяльність підприємства. Наступним критичним кроком є виявлення вразливих місць у системі безпеки. Це точки, які можуть використовуватися зловмисниками для доступу до конфіденційної інформації [17]. Оцінка таких вразливостей дозволяє компанії обрати оптимальні заходи для покращення захисту.

Соціальні вразливості стосуються всіх процесів, пов'язаних з маніпулюванням персоналом для отримання несанкціонованого доступу до інформації або систем. Методи соціальної інженерії можуть застосовуватися для обману працівників з метою отримання конфіденційної інформації або доступу до систем [1].

Юридичні вразливості виникають через недоліки в правовому забезпеченні захисту даних. Причиною цього виявляється відсутність чітких політик конфіденційності або регуляторних норм, що призводять до невизначеності прав і обов’язків у сфері зберігання даних та захисту інтелектуальної власності [1].

Сформовані методи захисту КТ представлений на рисунку 1.2.

Рис. 1.2. Сформовані методи захисту КТ

Бізнес-вразливості включають ризики, пов’язані з організаційними процесами, які можуть використовуватись для впровадження загроз. Недоліки у ризик-менеджменті можуть призводити до невірної оцінки ризиків безпеки, ускладнювати пріоритети у сфері захисту або зменшувати ресурси на безпеку. Крім того, неналежний контроль над постачальниками може стати джерелом небезпек через слабкість їхніх систем або неналежну передачу конфіденційної інформації.

Після виявлення загроз та вразливостей необхідно провести оцінку ризиків, щоб оцінити ймовірність виникнення інцидентів безпеки та їхні можливі наслідки [2]. На основі цього аналізу розробляються заходи, які допоможуть знизити ризики та забезпечити належний захист комерційної інформації.

Планування захисних заходів включає розробку стратегій, процедур і технологій, що забезпечують конфіденційність даних компанії та запобігають потенційним загрозам. Важливо охопити технічні, організаційні та правові сторони безпеки [2].

Перш за все, необхідно провести аудит безпеки, щоб оцінити поточний рівень захисту і виявити потенційні слабкі місця. Що дозволить розробити стратегії для їх усунення.

Наступним кроком є створення політики захисту комерційної таємниці, що визначає правила, яких повинні дотримуватися усі працівники компанії. Така політика повинна охоплювати правила доступу до конфіденційної інформації, обміну даними та механізми захисту від несанкціонованого доступу.

Одношевна О.О., Вітер В.А. та Калмиков С.О. пишуть: «Проблема шахрайства полягає не лише у прямих фінансових збитках, але й у довготривалих негативних наслідках для підприємства» [34]. Також у науковій праці наголошують: «Ризики шахрайства впливають на всі аспекти діяльності підприємства, включно з управлінням ресурсами, стратегією розвитку та інвестиційними рішеннями» [34].

Необхідно проводити регулярне навчання персоналу щодо правил кібербезпеки та поводження з конфіденційною інформацією. Для організації такого процесу необхідно включати тренінги з протидії кібератакам, ознайомлення з процедурами реагування на інциденти безпеки та інші навчальні програми.

Технічні заходи також потребують значної уваги, включаючи встановлення та підтримку спеціального програмного забезпечення для захисту даних, використання фаєрволів, системи виявлення вторгнень, а також своєчасне оновлення програм для усунення вразливостей [51].

Не менш важливим є моніторинг та аудит безпеки, що дозволяє своєчасно виявляти загрози та вживати заходів ще до того, як вони переростуть у серйозні проблеми для підприємства.

Загалом, для забезпечення надійного захисту комерційної таємниці необхідний комплексний підхід, що охоплює широкий спектр заходів від технічних до організаційних. Реалізація цих заходів дозволяє компанії мінімізувати ризики витоку інформації та забезпечити стабільний захист даних.

1.3 Досвід захисту комерційної таємниці та важливих даних з вітчизняних та зарубіжних джерел

Управління КТ – це важливий напрямок для підприємств як в Україні, так і за кордоном. На тлі зростаючих кіберзагроз і конкуренції на ринку, вивчення національних та міжнародних підходів у цій сфері стає актуальною задачею для компаній, що прагнуть забезпечити надійний захист своєї інформації.

Вітчизняний досвід управління КТ формується з урахуванням національного законодавства, стратегій кібербезпеки та практичних заходів, які реалізують українські підприємства. Законодавча база України містить положення щодо захисту комерційної інформації, це відбувається через Закон «Про захист інформації в інформаційно-телекомунікаційних системах» [42].

Закон створює правові основи для захисту конфіденційної інформації від незаконного доступу, використання та розголошення в межах інформаційно-телекомунікаційних систем. Визначає обов’язки господарюючих суб’єктів у захисті комерційної інформації, яка має цінність для власника та підлягає захисту. Механізми, закріплені в законі, включають правила доступу, захист інформації при її передачі та зберіганні, а також відповідальність за порушення цих вимог. Для контролю за дотриманням цих вимог проводяться аудити та інспекції.

Зарубіжний досвід, зокрема американський, демонструє ефективні підходи до управління КТ. Закон "Про захист торговельної таємниці" (Defend Trade Secrets Act), прийнятий у США в 2016 році, унормовує визначення торговельної таємниці на федеральному рівні, захищаючи широкий спектр технічної, комерційної та фінансової інформації. Закон дозволяє компаніям звертатися до суду у випадках порушення таємниці та відшкодовувати збитки, завдані незаконним доступом або розголошенням конфіденційної інформації [1].

Впровадження інноваційних технологій, штучного інтелекту та машинного навчання, дозволяє компаніям, таким як Google, Apple та Amazon, виявляти аномалії та потенційні загрози в режимі реального часу. Включає багаторівневі заходи, від архітектурних захисних рішень до контролю доступу та шифрування. Крім технічних рішень, у цих компаніях посилено працюють над управлінням ризиками, формуванням політик безпеки та навчанням співробітників у сфері кібербезпеки.

Ще одним напрямом зарубіжного досвіду є співпраця з провідними кібербезпековими компаніями, що забезпечує доступ до новітніх розробок та дозволяє своєчасно реагувати на нові загрози.

Підсумовуючи, вивчення і впровадження кращих національних та зарубіжних практик з управління комерційною таємницею сприяє підвищенню ефективності захисту інформації. Українським компаніям

важливо стежити за новими методами управління ризиками, інтегруючи їх у свою діяльність та адаптуючи до національного законодавства для забезпечення максимального захисту конфіденційних даних.

Впровадження найкращих практик управління КТ, розроблених на основі як національного, так і міжнародного досвіду, дає українським компаніям змогу підвищити ефективність захисту конфіденційної інформації. За допомогою адаптації новітніх підходів до оцінки ризиків, кібербезпеки та внутрішніх політик до вимог національного законодавства, підприємства здатні мінімізувати вразливості у своїй діяльності. За допомогою використання таких підходів та аналізу сучасних проблем з різних джерел, можливо суттєво підвищувати рівень захисту даних на господарствах, постійно впроваджувати актуальні рішення з оновленнями реагуючи на нові джерела небезпек.

Висновки до першого розділу

1. Комерційна таємниця (КТ) є фундаментальним компонентом забезпечення економічної безпеки підприємств. Вона включає цінну інформацію, яка дозволяє компаніям утримувати унікальну ринкову позицію. За аналізом представлених літератур них джерел виявлено, що До КТ належать технологічні розробки, маркетингові стратегії, база клієнтів та інші дані, які сприяють збереженню конкурентних переваг. Зазначаю також що умовах швидкого інформаційного обміну захист КТ стає не лише питанням збереження активів, а й умовою стійкого розвитку бізнесу.

2. Далі у роботі висвітлено, що типи і форми КТ різняться залежно від галузі, специфіки діяльності підприємства та рівня її важливості для бізнесу що підтверджують і праці інших авторів які працюють у ці тематиці, а саме [28]. Зокрема, технічна інформація охоплює виробничі процеси, а фінансова

– структуру витрат і ціноутворення. Далі у своїй роботі я дослідив що маркетингові стратегії та ринкові прогнози вимагають специфічного підходу до захисту, оскільки їхня втрата може завдати непоправних збитків компанії. Рекомендовано взяти до уваги що, індивідуальний підхід до визначення критичних аспектів КТ дозволяє підвищити ефективність захисних заходів.

3. Виявлено основні загрози збереженню конфіденційності КТ охоплюють кіберзлочинність, технічні недоліки, людський фактор і недостатній рівень правового захисту. З літературного аналізу визначено що особливу небезпеку становлять прогалини в кіберзахисті, застаріле програмне забезпечення, слабкі паролі чи недостатнє навчання персоналу. Рекомендовано звертати увагу на скільки важливим є системний підхід до ідентифікації ризиків і розробки стратегій їхнього управління.

4. У дослідженні доведено, що надійний захист КТ базується на поєднанні технічних, організаційних і юридичних заходів. У розрізі першого розділу виявлено що важливу роль відіграють методи шифрування, багаторівнева аутентифікація, впровадження фаєрволів і регулярне оновлення програмного забезпечення як зазначають і інші дослідники з цієї сфери. Організаційні заходи включають політики доступу, навчання персоналу та проведення регулярних аудитів безпеки, тоді як юридичні – угоди про нерозголошення (NDA) і реєстрацію інтелектуальної власності.

5. У роботі досліджено із відкритих джерел та акцентовано увагу на важливості національного законодавства у формуванні політик конфіденційності. Для захисту КТ підприємствам необхідно враховувати вимоги законів України, зокрема Закону «Про інформацію» та нормативних актів, що регулюють порядок роботи з конфіденційними даними, особисто рекомендується не втрачати з уваги цей правовий акт. Систематична адаптація законодавчих норм я досліджено раніше, забезпечує до сучасних загроз надійний правовий захист підприємств.

6. Проаналізовано з літератури та описано у розділі, як проводиться ідентифікація загроз, таких як кіберзлочинність, витік даних через людський фактор або недоліки фізичної безпеки. Описаний підхід дозволяє підприємствам оцінити можливий вплив цих ризиків на бізнес-процеси. Управління ризиками, охоплює розробку стратегій пріоритетного захисту вразливих даних, з мого особистого спостереження та дослідження виявлено такий підхід забезпечує оптимізацію ресурсів і знижує потенційні збитки.

7. Також з проведених досліджень та аналізу робіт авторів зазначених у посиланнях, у цьому розділі мною запропоновано впровадження інноваційне рішення щодо сучасних гібридних технологій шифрування, що поєднують асиметричні алгоритми (RSA, ECC) для захисту ключів із симетричним алгоритмом AES для шифрування основних даних, за якими методиками вони працюють було досліджено з навчальної літератури. Також рекомендовано впровадження системи моніторингу вхідних повідомлень на предмет фішингових загроз. Рекомендаціями буде використання комплексного підходу до захисту даних що дозволить підприємствам підвищити рівень безпеки та запобігти витоку критичної інформації.

РОЗДІЛ 2. ПРОВЕДЕННЯ АНАЛІЗУ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ТОВ АГРОФІРМА «СЛАВУТИЧ»

2.1 Характеристика фінансово економічної діяльності ТОВ Агрофірма «Славутич»

З зібраної інформації під час проходження практики виявлено ТОВ Агрофірма «Славутич» (код ЄДРПОУ 25520143) була заснована 21 квітня 1998 року як товариство з обмеженою відповідальністю. Станом на 1 листопада 2024 року юридична особа має статус «зареєстровано», а її статутний капітал складає 30 000 грн. Головою підприємства виступає Браціло Роман Володимирович, який також є уповноваженою особою компанії.

Компанія «Славутич» займається виробництвом різноманітної сільськогосподарської продукції. Основний напрямок діяльності – вирощування зернових і бобових культур, а також насіння олійних культур (КВЕД 01.11). Окрім цього, підприємство вирощує плодові культури (зокрема зерняткові та кісточкові), розводить свиней та виконує допоміжну діяльність у сфері рослинництва. Юридична адреса ТОВ Агрофірма «Славутич» – Дніпропетровська область, Синельниківський район, село Катеринівка, вул. Центральна. У організаційній структурі управління ТОВ Агрофірма «Славутич» не передбачено окремого відділу економічної безпеки. Обов'язки з забезпечення захисту економічних інтересів компанії покладаються на керівників основних внутрішніх підрозділів, які здійснюють контроль у межах своїх повноважень.

З зібраних матеріалів під час практики встановлено що майновий фонд компанії формується з декількох джерел, серед яких внески засновників до

статутного капіталу, прибуток від продажу аграрної продукції, банківські кредити, а також можливе залучення фінансів через випуск цінних паперів. Також було виявлено що підприємство має напрямки інші доступні фінансові інструменти для збільшення капіталу та розширення виробничих можливостей. Схема управління підприємством представлена на рисунку 2.1.

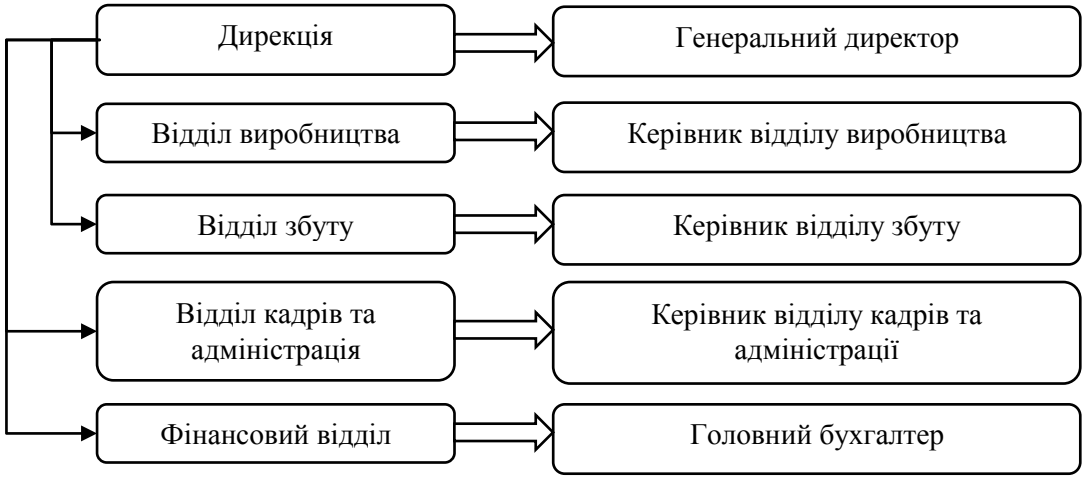

Рис. 2.1. Схема управління підприємством

Протягом останнього періоду проходження практики був проведений аналіз стану активів товариства, який показав їхню динаміку та надав актуальну оцінку майна компанії. Отримані результати подано на рисунку 2.2, що дозволяє наочно простежити зміни у вартості активів та визначити ефективність використання ресурсів.

Запаси також зазнали значних змін: у 2023 році вони зросли на 49% порівняно з 2019 роком. Основними факторами, що вплинули на збільшення запасів, стали зростання закупівельної вартості сировини та матеріалів. Суттєвий вплив мали інфляційні процеси які спостерігаються в Україні, коливання курсу національної валюти, підвищення транспортних витрат та нестабільність на ринку постачальників. Оборотні активи показали зниження у 2023 році, порівняно з початковим рівнем у 2019 році як було розраховано. Зміна пов'язана з оптимізацією запасів та зниженням рівня дебіторської заборгованості компанії. Нестабільність цього показника також вказує на

коливання в оборотних коштах, через це з'являться потреба постійного моніторингу змін у цьому напрямку.

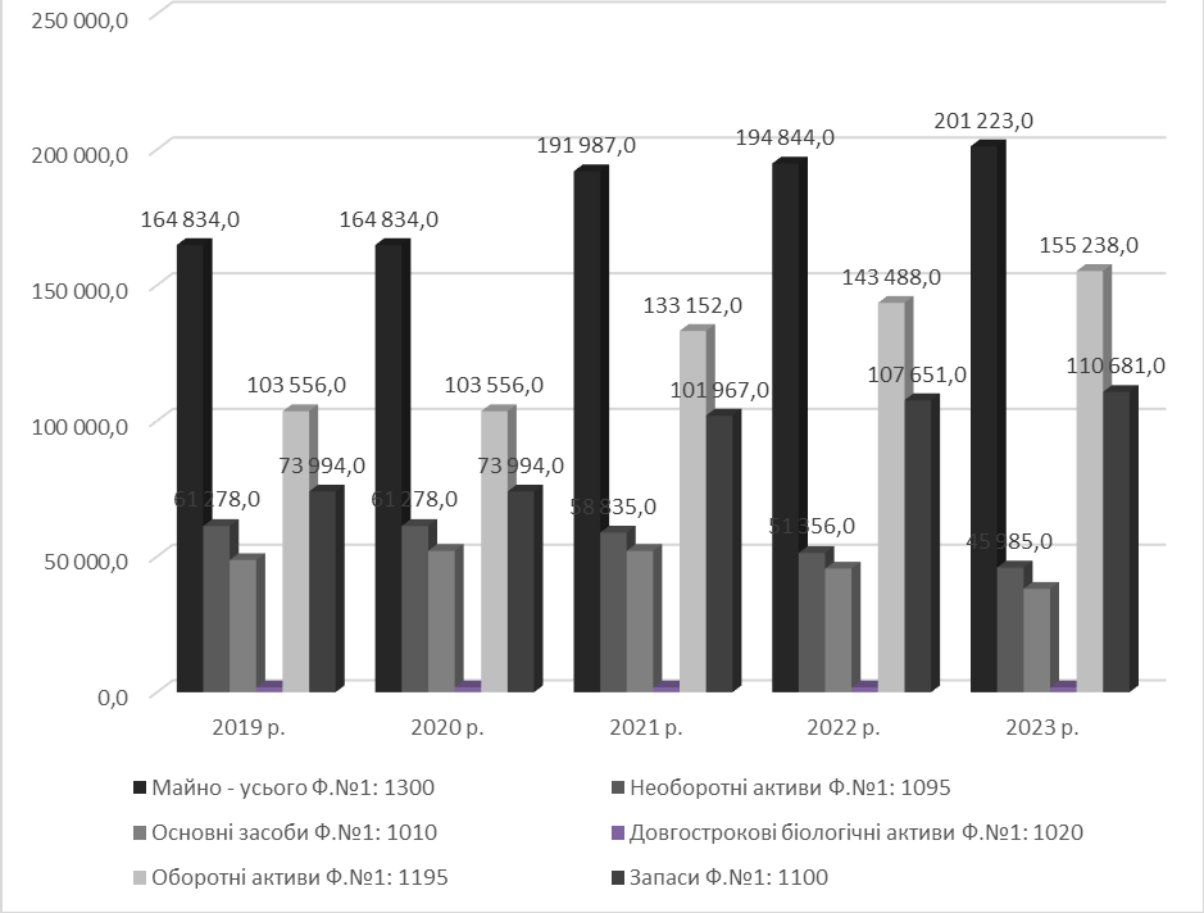

Рис.2.2 Зміна майна в ТОВ Агрофірма «Славутич» за 2019-2023 рр.

За отриманими даними проведено узагальнення що у 2023 році вартість необоротних активів зросла на 59% у порівнянні з 2019 роком. Збільшення було спричинене дооцінкою активів до їхньої ринкової вартості, а також оновленням та модернізацією частини основних засобів для покращення виробничих процесів.

У структурі довгострокових біологічних активів виявлені зміни. Показники залишалися стабільними до 2021 року, але у 2022 році відбулося різке зниження, і на 2023 рік цей показник взагалі відсутній. Було встановлено з даного аналізу, що компанія зробила відмову від довгострокових біологічних активів для способу розвитку. За власними спостереженнями структура власного капіталу підприємства залишалася стабільною протягом аналізованого періоду з 2019 рік по 2023 рік, що

свідчить про відсутність суттєвих змін у політиці компанії щодо нарощування власного капіталу. В умовах нинішньої економічної ситуації мною виявлено що підприємство обрало консервативну стратегію, зосереджуючи увагу на підтриманні існуючого рівня капіталу.

Далі я проводив аналіз основних засобів. Вони є основою матеріально-технічної бази підприємства. З літератури та практикумів встановлено що основних засобів належать транспортні засоби, сільськогосподарське обладнання, устаткування для обробки та зберігання продукції, а також будівлі, такі як адміністративні та складські приміщення.

Ефективність використання основних засобів найкраще оцінювати за допомогою коефіцієнтів зносу та придатності, які відображені на рисунку 2.3.

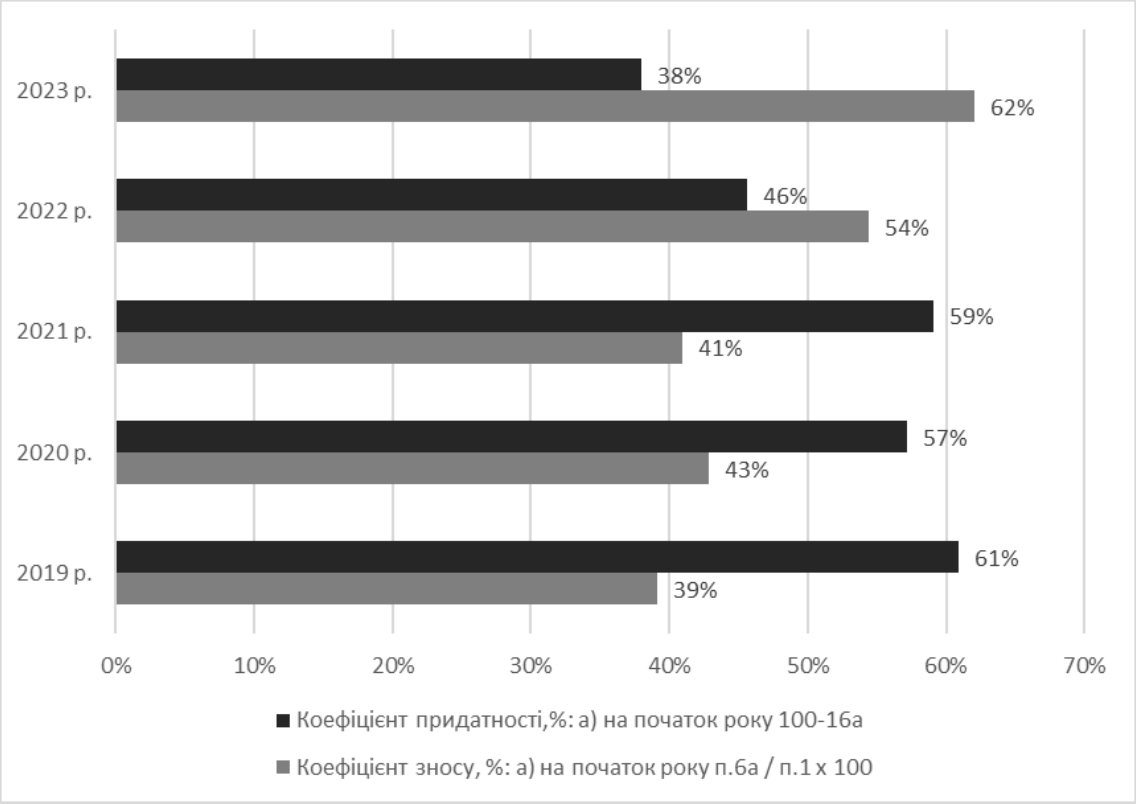

Рис. 2.3 Діаграма використання основних засобів в ТОВ Агрофірма «Славутич» за 2019-2023 рр.

При власному аналізі діаграми використання основних засобів, можна відзначити деякі тенденції. Спостерігається поступове збільшення коефіцієнту зносу, що вказує на зростання частки зношених основних засобів

підприємства. Цей показник зріс з 39% у 2019 році до 62% у 2023 році, у розрізі дослідження я визначаю це як активне старіння та зношення основних засобів за аналізований період. Виявлено з досліджених матеріалів що пов'язано це з недостатністю оновлення технічного парку підприємства, що призводить до збільшення зношення вже наявних активів. Фахівці з цієї сфери досліджень наголошують що така ситуація може негативно вплинути на продуктивність підприємства в довгостроковій перспективі, оскільки збільшення зносу зазвичай призводить до збільшення витрат на ремонт та обслуговування.

Щодо коефіцієнту придатності основних засобів, можна побачити зворотну тенденцію: він поступово знижується з 61% у 2019 році до 38% у 2023 році. Вказує це на зменшення залишкової вартості основних засобів підприємства порівняно з їх первісною вартістю, що може вказувати на необхідність значного оновлення технічних ресурсів. Також це говорить що частка основних засобів, придатних для експлуатації, зменшується, що в майбутньому може вплинути на здатність підприємства підтримувати стабільні обсяги виробництва.

Загалом, за власними проведеними дослідженнями у цьому напрямку, результати аналізу вказують на погіршення технічного стану основних засобів за останні п'ять років. Дається порада що підприємству доцільно розглянути можливість оновлення або модернізації основних засобів, фахівці підтверджують що це сприятиме підвищенню їхньої продуктивності та зменшенню витрат на обслуговування.

Наступним кроком слід провести аналіз доходів від реалізації продукції, дані наведені на рисунку 2.4.

З 2019 до 2020 року чистий дохід знизився з 89,410.0 тис. грн до 87,821.0 тис. грн, що становить зменшення приблизно на 1.8%. З 2020 до 2021 року відбувся значний спад доходу до 69,077.0 тис. грн, що є зменшенням приблизно на 21.3% порівняно з попереднім роком. У 2022 році

чистий дохід збільшився до 88,294.0 тис. грн, що становить зростання на 27.8% порівняно з 2021 роком. У 2023 році дохід знизився до 79,930.0 тис. грн, що становить спад на 9.5% порівняно з попереднім роком.

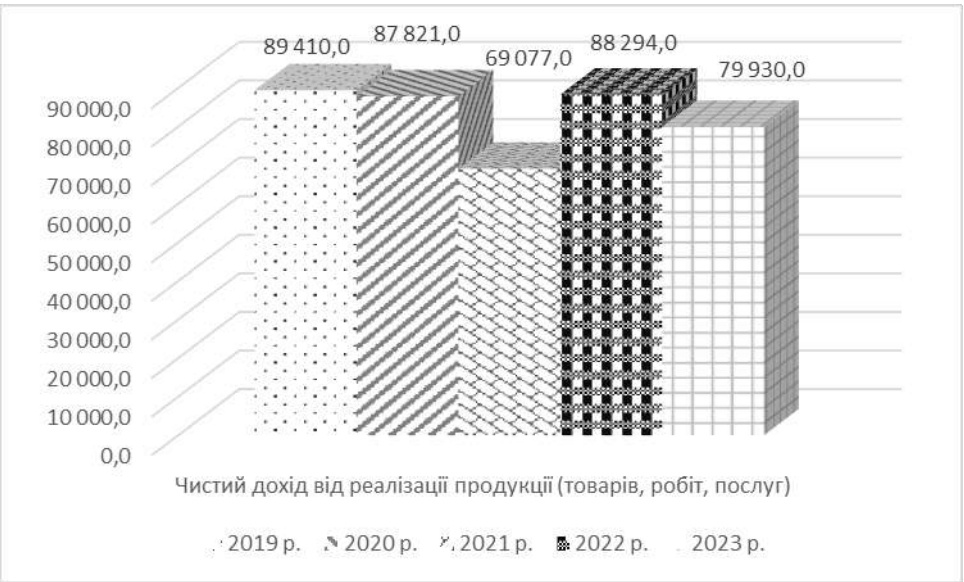

Рис. 2.4 Діаграма змін чистого доходу від реалізації продуктів та послуг в ТОВ Агрофірма «Славутич»

Динаміка змін чистого доходу ТОВ Агрофірма «Славутич» за період 2019-2023 років демонструє нестабільність з певними коливаннями, що, ймовірно, пов'язані з ринковими умовами та внутрішніми процесами підприємства. Виявлено з аналізу що основним викликом став спад 2021 року, проте швидке відновлення у 2022 році говорить про адаптивність та ефективність реакції компанії на виклики. Незважаючи на спад у 2023 році, дохід залишається достатньо високим, що вказує на потенціал для стабілізації та подальшого зростання при умові підтримки ефективної стратегії управління та гнучкості до змін у ринкових умовах.

Далі розглянемо витрати на операційну діяльність, дані наведені на рисунку 2.5.

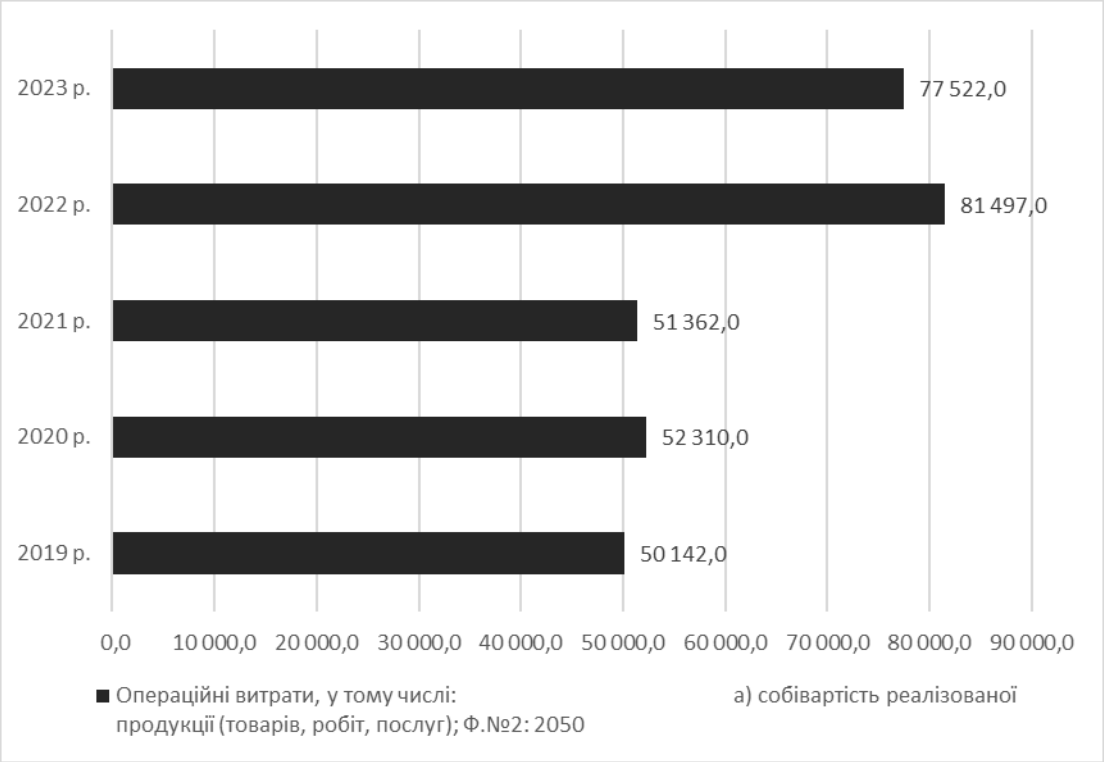

Рис. 2.5 Діаграма витрат на операційну діяльність

За моїм аналізом, з 2019 до 2020 року операційні витрати зросли з 50,142.0 тис. грн у 2019 році до 52,311.0 тис. грн у 2020 році, що становить приріст приблизно на 4.3%. У 2021 році витрати зменшилися до 51,362.0 тис. грн, що становить зниження приблизно на 1.8% порівняно з попереднім роком. У 2022 році операційні витрати зросли до 81,497.0 тис. грн, що є значним збільшенням на 58.7% порівняно з попереднім роком. У 2023 році витрати зменшилися до 77,522.0 тис. грн, що є спадом на 4.9% порівняно з 2022 роком.

Динаміка операційних витрат ТОВ Агрофірма «Славутич» за 2019-2023 роки демонструє як помірне зростання, так і різке збільшення витрат у 2022 році, що було пов'язане з нестабільною економічною ситуацією та збільшенням цін на ресурси. Спроби оптимізації витрат у 2021 і 2023 роках вказують на прагнення компанії утримувати витрати під контролем, але високі витрати 2022 року підкреслюють потребу в подальших заходах для стабілізації собівартості реалізованої продукції.

Наступним стає дослідження валового та чистого прибутку. Дані з цього показника зображені на рисунку 2.6.

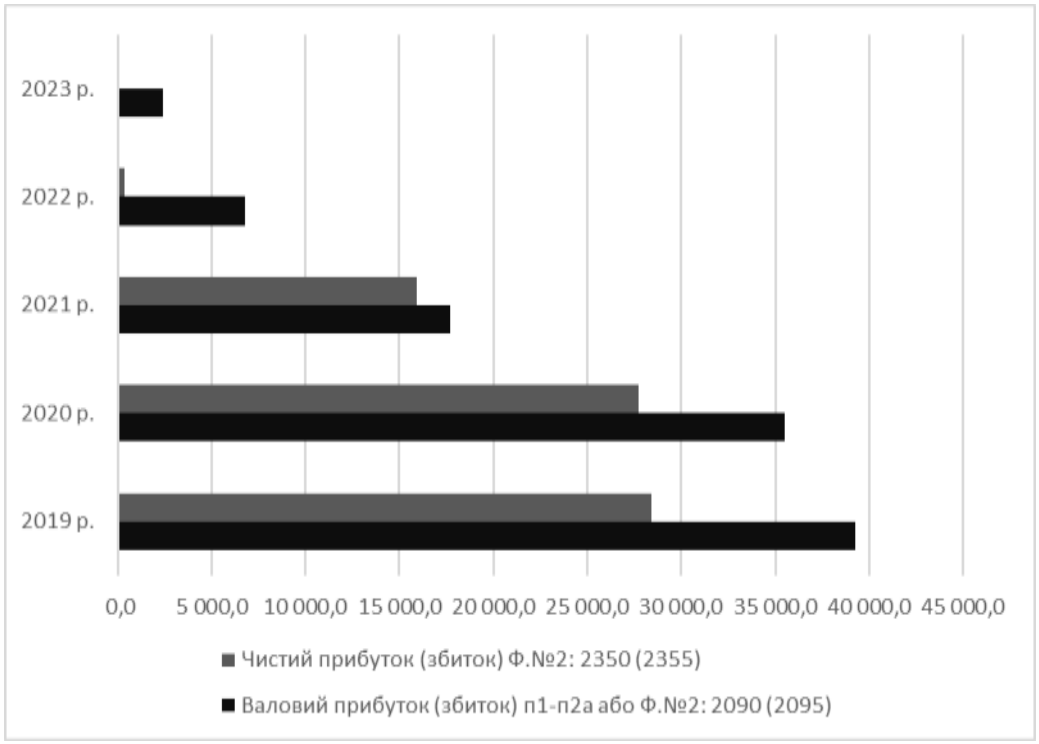

Рис. 2.6. Дослідження зміни валового та чистого прибутку в ТОВ Агрофірма «Славутич» за 2019-2023 рр.

За аналізом мого спостереження з графіків, загальна динаміка показує стабільність у перші два роки з подальшим різким зниженням як валового, так і чистого прибутку з 2021 року. За період з 2019 до 2023 року валовий прибуток зменшився приблизно на 95%, а чистий прибуток – на понад 99%. Така тенденція вказує на серйозне зниження фінансової стабільності підприємства та необхідність перегляду стратегії для виходу з кризової ситуації.

Даля я провів оцінку фінансової стабільності підприємства ТОВ Агрофірма «Славутич» брав до уваги аналіз коефіцієнтів автономії та довгострокового залучення позикових коштів. Зазначаю що коефіцієнт автономії, відображає частку власного капіталу в загальній структурі капіталу підприємства. Оптимальне значення цього коефіцієнта має перевищувати 0,5, що свідчить про фінансову незалежність компанії. З аналізу цього питання говориться що високий рівень автономії дозволяє

підприємству забезпечувати свою діяльність власними ресурсами, а також це дає перевагу мінімізувати залежність компанії від використання позикових коштів.

За аналізований період з 2019 до 2023 року спостерігається поступове зниження коефіцієнта автономії. У 2019 році цей показник був близько 99,5%, що свідчить про високий рівень фінансової незалежності. Проте у 2022 році коефіцієнт автономії значно знизився, опустившись до 98%, а у 2023 році він дещо покращився, але все ще залишався нижче показників початку періоду.

Коефіцієнт довгострокового залучення позикових коштів, протягом усього аналізованого періоду залишався на рівні 100%. З аналізу та досліджень вказує це на стабільно високий рівень залучених позикових коштів у структурі капіталу підприємства, на мій погляд та погляд фахівців з даного напрямку вказує це на значну залежність від зовнішнього фінансування.

Сукупний аналіз цих показників демонструє, що підприємство підтримує високий рівень позикових коштів при дещо зниженому рівні власного капіталу. Діаграма автономії підприємства зображена на рисунку 2.7.

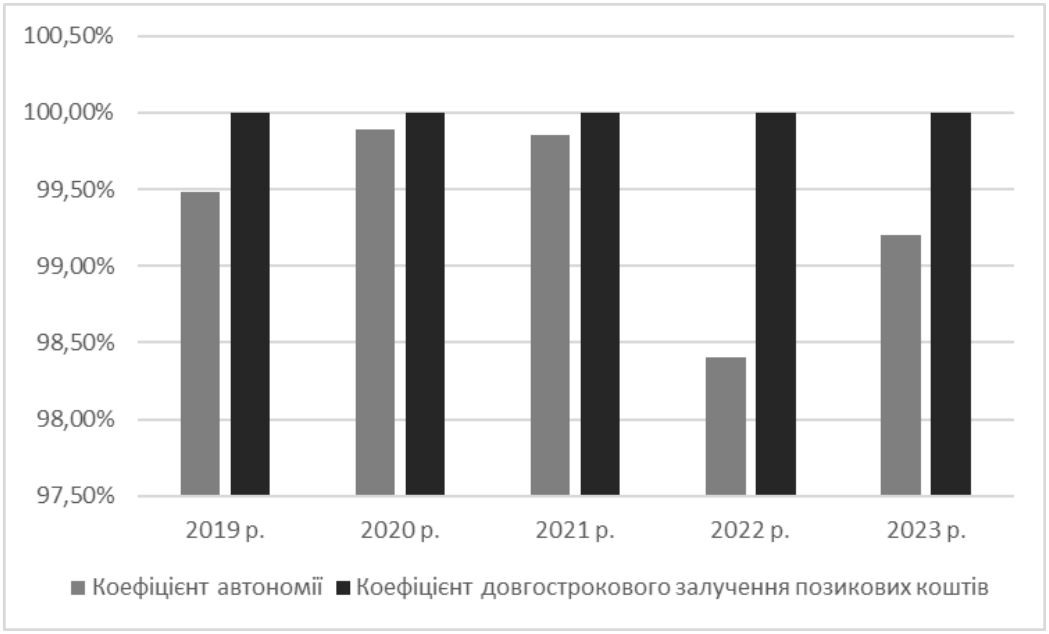

Рис. 2.7 Діаграма зміни коефіцієнта автономії і довгострокового залучення позики в ТОВ Агрофірма «Славутич» за 2019-2023 рр.

На заключному етапі аналізу розглянемо показники ділової активності. Проведемо аналіз таких показників, як фондовіддача необоротних активів, коефіцієнт оборотності капіталу, тривалість одного обороту оборотних активів, а також періоди оборотності дебіторської та кредиторської заборгованості. При оцінці ділової активності особливу увагу приділимо показникам, що характеризують тривалість обороту дебіторської та кредиторської заборгованості, оскільки вони впливають на рівень ліквідності та фінансову стійкість підприємства.

Діаграма оцінки динаміки обертання активів наведена на рисунку 2.8. Коефіцієнт оборотності оборотних активів демонструє, наскільки ефективно підприємство використовує свої оборотні активи для отримання доходу. У 2019 році цей показник становив 86,47%, що свідчить про досить високу активність. Проте у 2020 році він дещо зменшився до 84,81%, що може свідчити про зниження ефективності використання оборотних активів. У наступні роки спостерігається помітне зниження цього показника до 53,51% у 2023 році.

Коефіцієнт завантаження оборотних активів показує, яка частка активів підприємства використовується у його операційній діяльності. У 2019 році він становив 115,65%, що є прийнятним значенням, яке вказує на збалансоване використання активів.

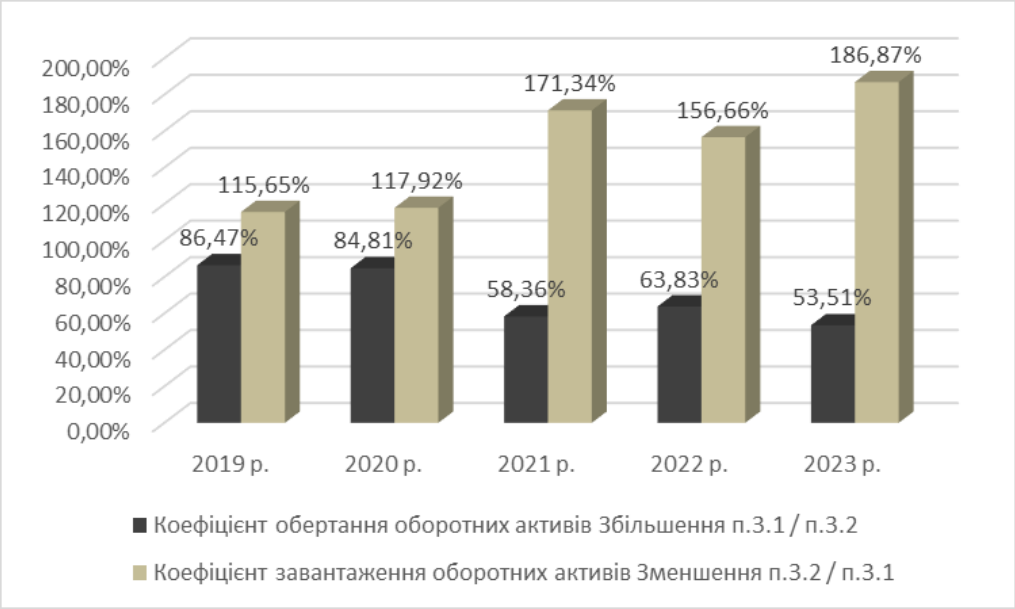

Рис. 2.8 Аналіз динаміки показників оборотності в ТОВ Агрофірма «Славутич» за 2019-2023 рр.

Проте вже з 2021 року спостерігається різке зростання цього коефіцієнта до 171,34%, а у 2023 році він досягає максимального значення – 186,87%. Це вказує на підвищене навантаження на активи, спричинено необхідністю збільшення обсягу короткострокового фінансування.

Загалом, аналіз показує, що протягом 2019–2023 років відбулося зниження коефіцієнта оборотності оборотних активів, що вказує на зниження швидкості обігу активів та свідчить про труднощі з ліквідністю. Одночасно коефіцієнт завантаження оборотних активів значно зріс, що свідчить про збільшення операційного навантаження на активи. Це є ознакою того, що підприємство стало більш залежним від позикових коштів, і для підтримки поточної діяльності необхідне додаткове фінансування.

2.2. Дослідження та оцінка роботи відділу економічної безпеки на підприємстві ТОВ Агрофірма «Славутич»

У сучасних умовах діяльність підприємства супроводжується численними викликами, і передбачити всі труднощі, що можуть виникнути, є

вкрай складно. Щоб забезпечити економічну безпеку, важливо швидко реагувати на зміни у фінансовому середовищі підприємства, зміни в законодавстві, ситуації на ринках збуту, а також соціальні та технологічні тенденції. Під час дослідження встановлено, що ТОВ Агрофірма "Славутич" застосовує сучасні технічні засоби та програмне забезпечення для ведення обліку й звітування в контролюючі органи.

На підприємстві наразі відсутній окремий відділ економічної безпеки, і вся відповідальність за забезпечення та захист економічної безпеки покладається на керівників структурних підрозділів. Зокрема, за фінансову діяльність, достовірність, збереження та захист джерел облікової інформації відповідає бухгалтерська служба під керівництвом головного бухгалтера.

Для підвищення ефективності системи економічної безпеки ТОВ Агрофірма "Славутич" доцільно розглянути можливість створення окремого підрозділу економічної безпеки. Основним кроком у цьому напрямку є визначення пріоритетних завдань і цілей, які така служба буде виконувати для забезпечення безперебійної діяльності підприємства. Перелік основних функцій, які має виконувати відділ економічної безпеки для ТОВ Агрофірма "Славутич" наведено на рисунку 2.9.

Значення управління економічною безпекою ТОВ Агрофірма «Славутич» визначається його ключовими функціями і завданнями. До основних завдань належать оцінка потенційних загроз для компанії, вжиття заходів для запобігання ризикам, розробка плану захисту від різних типів загроз, а також контроль за виконанням цих заходів для забезпечення своєчасного інформування керівництва.

Першим етапом подальшого дослідження є оцінка рівня складових фінансово-економічної безпеки ТОВ Агрофірма «Славутич». Розрахунки проводимо відповідно до положень «Методичних рекомендацій щодо діагностики рівня безпеки». Кожен елемент економічної безпеки аналізується

поступово, з використанням різних методів, зокрема проведення опитувань серед працівників підприємства.

На основі проведених розрахунків було отримано наступні результати:

Крок 1. Проведено оцінку фінансової складової економічної безпеки підприємства. Для розрахунків використано такі формули:

$$Ее = ВК - А1 \quad (2.1)$$

$$Ес = Ее - Z \quad (2.2)$$

Де: А1 – необоротні активи; ВК – власний капітал;

Z – розмір запасів;

$$Ее = 191137 - 45985 = 145152$$

$$\pm Ес = 145152 - 110681 = 34471$$

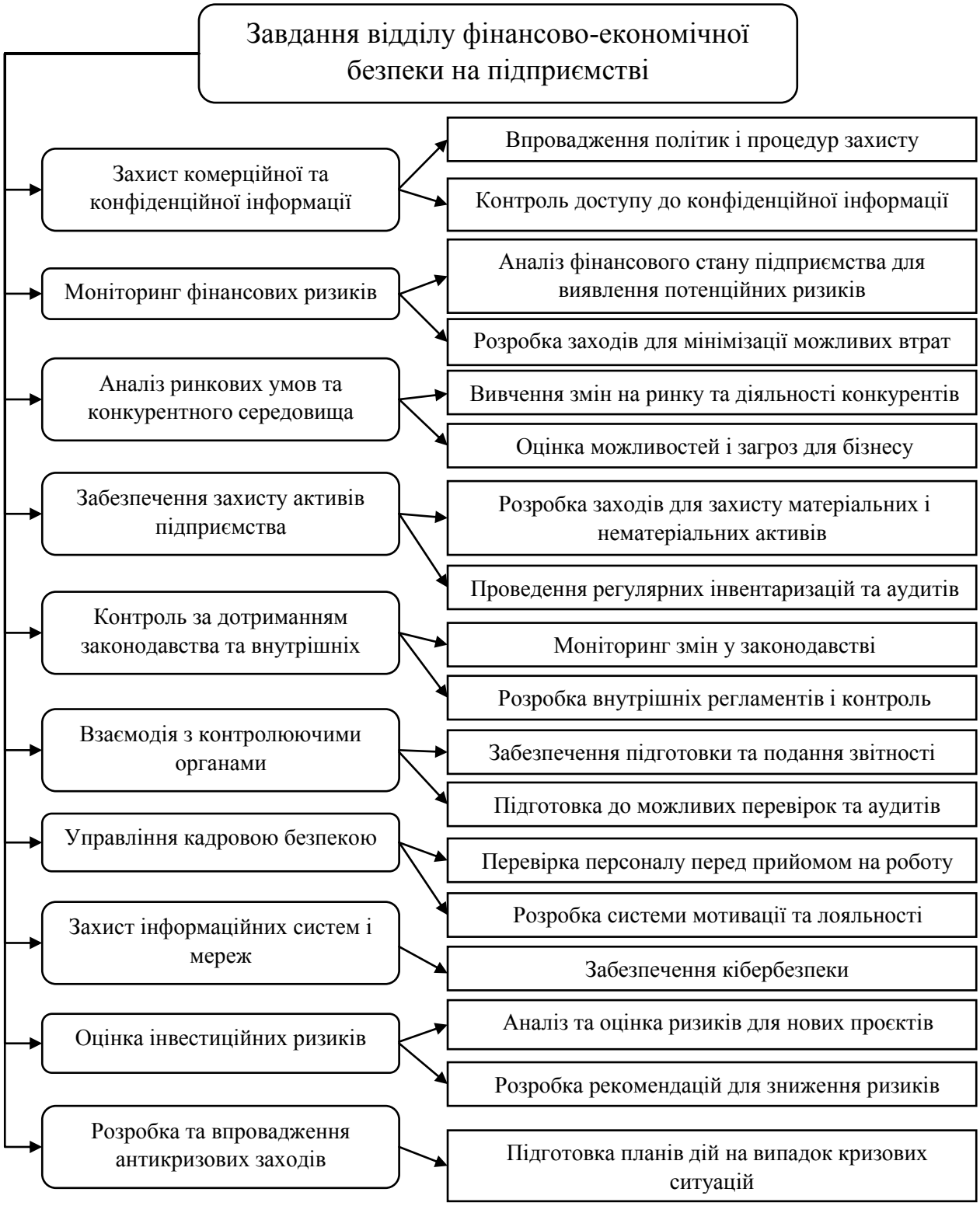

Рис. 2.9. Завдання відділу фінансової безпеки на підприємстві

Отримане значення показника вказує на те, що підприємству достатньо власних фінансових ресурсів для покриття витрат, необхідних для формування потрібного обсягу запасів.

±Ет – забезпечення підприємства власними обіговими коштами, а також залученими середньо- та довгостроковими кредитами (К):

$$\pm Ет = (Ее + К) - Z \quad (2.3)$$

Де: К – це довгострокові зобов'язання;

$$\pm Ет = (145152 + 0) - 110681 = 34471$$

Результат даного показника демонструє що на підприємстві достатньої кількості власних коштів, середньострокових і короткострокових позик.

±Ен забезпечення підприємства власними обіговими коштами, а також коротко-, середньо- та довгостроковими кредитами і позиками (Кт):

$$\pm Ен = (Ее + Кт + К) - Z \quad (2.4)$$

Де: Кт - це короткострокові кредити банків

$$\pm Ен = (145152 + 0 + 0) - 110681 = 34471$$

Результат цього показника свідчить, що підприємство володіє достатнім рівнем власних коштів для покриття витрат на закупівлю та формування запасів.

Аналіз фінансових показників також показує, що компанія не використовує короткострокові кредити у своїй поточній діяльності, що свідчить про належний рівень фінансової стійкості. Показники фінансової безпеки підприємства мають такі значення: ±Ес (34471) > 0, ±Ет (34471) > 0, ±Ен (34471) ≥ 0.

Відповідно до методології оцінки, умовно надаємо цьому стану абсолютне значення 4, що відображає задовільний рівень фінансової стабільності, зумовлений наявністю обмежених оборотних коштів для покриття витрат і підтримки запасів.

Крок 2. Оцінено рівень інформаційної складової економічної безпеки. Розраховано такі показники:

Коефіцієнт інформаційної повноти (Кп):

$$Кп = Кз / Кгр = 0{,}78 \quad (2.5)$$

Коефіцієнт достовірності інформації (Кт):

$$Кт = Кр\ /Кз = \ 0{,}79 \quad (2.6)$$

Коефіцієнт неточності інформації (Кс):

$$Кт = Кнс\ /Кнср = \ 0{,}58 \quad (2.7)$$

Рівень інформаційної безпеки обчислюється як добуток відповідних коефіцієнтів:

$$Кіб \ = \ Кп * \ Кс * \ Кт \ \ = \ 0{,}357 \quad (2.8)$$

Існують три рівні оцінки інформаційної безпеки:

- Високий – за значення Кіб ≥ 0,7
- Середній – при 0,3 ≤ Кіб < 0,7
- Низький – коли Кіб < 0,3

З огляду на те, що коефіцієнт інформаційної безпеки для нашого підприємства становить 0,357 для розрахунку загального показника присвоюємо йому абсолютне значення 2, що відповідає середньому рівню.

Крок 3. Проведено оцінку інтелектуальної складової економічної безпеки підприємства, використовуючи такі показники:

Коефіцієнт який враховує кваліфікацію працівників (Ккв):

$$Ккв = \frac{\sum_{i=1}^{n} У}{0} \quad (2.9)$$

Де: $\sum_{i=1}^{n} У$ це загальна величина рівня кваліфікації та освіти персоналу, а саме кількість працівників із вищою та середньою освітою;

О – загальна кількість працівників підприємства;

$k_{іо}$ - коефіцієнт інтелектуального забезпечення (Кіо);

$$k_{іо} = \frac{В_{ін}}{0} \quad (2.10)$$

Де: $В_{ін}$ це вартість інтелектуальної власності, що включає винаходи, бренди, товарні знаки, корисні моделі, раціоналізаторські пропозиції та різноманітні «ноу-хау», є важливим елементом сучасного бізнесу.

Для оцінки ефективності використання цієї власності розраховується норма доходності співробітників підприємства (Кд), що виражається в тисячах гривень:

$$k_{д} = \frac{Д_{іп}}{0} \quad (2.11)$$

Де: $Д_{іп}$ це отриманий дохід підприємства від використання інтелектуального потенціалу є важливим показником його фінансової ефективності.

Вагу кожного коефіцієнта визначають на основі експертних оцінок управлінського персоналу. Для сільськогосподарських підприємств застосовують такі коефіцієнти: Ккв – 0,5, Кіо – 0,25, Кд – 0,25.

Під час розрахунків коефіцієнтів кваліфікації працівників (1,7), коефіцієнта норми доходності (0,29) і інтелектуальної озброєності (0,38) було проаналізовано порогові значення показників, що слугують індикаторами рівня інтелектуальної безпеки підприємства. В результаті цього аналізу підприємству було присвоєно значення 2, що вказує на середній рівень інтелектуальної безпеки.

Крок 4. Виконаний аналіз кадрів як фінансово-економічної складової, за такими складовими:

Коефіцієнт плинності кадрів ($k_{п}$):

$$k_{п} = \frac{\Sigma^{Ч_{у}}}{О} = 5/77=0,064 \quad (2.12)$$

де $Ч_{у}$ - це кількість працівників, які були звільнені або скорочені протягом розрахункового періоду;

О - загальна чисельність працівників підприємства за той же період.

Коефіцієнт фізичного старіння кадрів (Кв):

$$k_{в} = \frac{О_{в}}{О} = 14/77 = 0,18 \quad (2.13)$$

Де: Ов — кількість працівників, які мають значний вік і відповідну кваліфікацію;

3. Фондоозброєність працівників (Фо) складає 455,50 тис. грн;

4. Фондоозброєність показників невиробничих фондів підприємства (Фно) становить 104,76 тис. грн.

Використовуючи зведену таблицю порогових значень показників кадрової безпеки, яка поділяється на чотири рівні, ми присвоюємо кадровій складовій значення 3, що свідчить про досягнення рівня задовільної безпеки.

Крок 5. Проведено оцінку рівня технологічної складової економічної безпеки підприємства. Використовуючи формулу середньозваженого значення та враховуючи коефіцієнти для сільськогосподарських господарств ($К_{п.прод}$ – 0,25; $К_{п.т}$ – 0,5; $К_{пат.прод}$ – 0,25), було визначено рівень техніко-технологічної безпеки. За розрахованим коефіцієнтом підприємству присвоєно абсолютне значення 3, що вказує на задовільний рівень безпеки в технологічній сфері.

Крок 6. Оцінка рівня правової складової економічної безпеки підприємства була проведена за допомогою аналізу показників, які поділяються на три категорії: абсолютний, задовільний та критичний. При розрахунках були використані такі вагові коефіцієнти, для сільськогосподарських підприємств: $К_п$ *– 0,25;* $К_в$ *– 0,2;* $Ф_о$ *– 0,35;* $Ф_{но}$ *– 0,2*. В результаті розрахунків було отримано коефіцієнт 3, що свідчить про абсолютний рівень правової безпеки на підприємстві.

Крок 7. Оцінка рівня екологічної складової економічної безпеки підприємства була проведена, і отримані результати виглядають наступним чином:

Для розрахунку коефіцієнта безпечності продукції ($k_{бп}$) була використана формула:

$$k_{бп} = \frac{Пс}{ПЗ} \qquad (2.14)$$

Де: Пс - виручка від реалізації сертифікованої продукції (грн);

Пз - загальна виручка від реалізації продукції (грн).

Коефіцієнт захисту середовища ($k_{зах}$) розраховується за формулою:

$$К_{зах} = \frac{В_{ек.з}}{В_з} \quad (2.15)$$

де $В_{ек}$ — витрати на екологію (грн);

$В_з$ — загальна сума витрат підприємства (грн).

Показники що стосуються екологічної безпеки господарства класифікуються на два рівні: задовільний та незадовільний. При задовільному рівні безпеки підприємству присвоюється значення 2, а при незадовільному — 1.

Було використано формулу середньозваженої оцінки для визначення рівня екологічної безпеки, порівнявши його із загальним коефіцієнтом. Для сільськогосподарських підприємств застосовуються наступні коефіцієнти: *$К_{б.п}$ - 0,5; $К_{зах}$ - 0,25*; *$К_з$ - 0,25;*

Розраховані показники екологічної складової свідчать про її задовільний стан, внаслідок чого їй присвоєно рівень 2.

Крок 8. Оцінка рівня силової складової економічної безпеки підприємства була проведена, зокрема, ці показники класифікуються на три категорії: високий, середній і низький. Для визначення рівня силової безпеки підприємства використано порогові індикатори та формулу середньої оцінки. У випадку сільськогосподарських підприємств використовуються наступні коефіцієнти: *$К_{сб}$ - 0,5 та $К_{в.ох.}$ - 0,5*. На основі проведеного аналізу силовій складовій було присвоєно абсолютне значення 2, що відповідає середньому рівню безпеки.

Крок 9. Визначаємо показник що відповідає загальному рівню фінансово-економічної безпеки ТОВ Агрофірма «Славутич», беручи до уваги відносну оцінку кожної складової безпеки. Відносна оцінка, визначається для кожної складової як співвідношення фактичного рівня економічної безпеки до максимально допустимого рівня цієї складової. Усі розрахунки представлені в таблиці 2.1.

Таблиця 2.1

Таблиця отриманих результатів економічної безпеки ТОВ Агрофірма «Славутич»

Складова ЕБ	***Фактичне значення***	***Максимальне значення***	***Відносна оцінка***
Інтелектуальна	2	4	0,50
Кадрова	3	4	0,75
Силова	2	3	0,67
Правова	3	3	1,00
Фінансова	4	5	0,80
Інформаційна	2	3	0,67
Технологічна	3	4	0,75
Екологічна	2	2	1,00

Зображаємо результати оцінки по кожній із складової економічної безпеки в ТОВ Агрофірма «Славутич», використовуючи діаграму на рисунку 2.10.

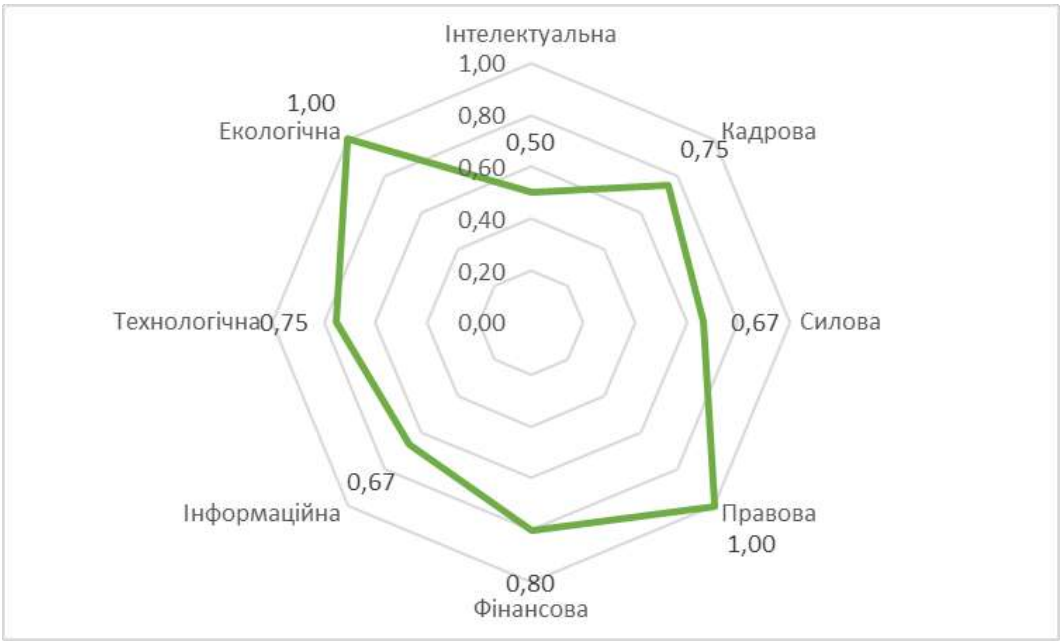

Рис. 2.10. Області економічної безпеки ТОВ Агрофірма «Славутич»

Аналізуючи надану діаграму економічної безпеки ТОВ "Агрофірма Славутич" станом на 2023 рік, можна зробити такі висновки. Враховуючи, що значення показника, ближче до одиниці, відображає високий рівень

економічної безпеки, а значення нижче 0,5 вказує на слабкий рівень, можемо оцінити стан основних складових.

Екологічна та Правова безпека мають найвищі значення (1,00), що вказує на відмінний рівень цих компонентів. Підприємство успішно дотримується екологічних стандартів і законодавчих вимог, що є важливим для його стабільної діяльності.

Інтелектуальна безпека знаходиться на середньому рівні (0,5), що говорить про середній стан знань, досвіду та інноваційних можливостей компанії.

Кадрова та Технологічна складові мають значення 0,75, що свідчить про достатній рівень, але є певний потенціал для покращення у цих напрямках. Підприємству варто продовжувати інвестувати в розвиток кадрів та удосконалення технологій. Фінансова безпека оцінена на рівні 0,80, що вказує на задовільну ситуацію з фінансовими ресурсами, але для більшої стабільності можливе посилення цієї складової. Інформаційна та Силова складові мають значення 0,67, що є нижчим за задовільний рівень.

За результатами аналізу вдалося дійти висновку що ТОВ Агрофірма «Славутич» демонструє добрий рівень економічної безпеки у більшості проаналізованих напрямків. Для забезпечення довгострокової стабільності та стійкості компанії на ринку, варто звернути додаткову увагу на покращення рівня таких елементів, як інформаційна та силова безпека. SWOT-аналіз ТОВ Агрофірма «Славутич» представлено у таблиці 2.2.

Розрахунок показника Альтмана для підприємства. Визначаємо за формулами:

$$Z = 0.717 * X_1 + 0.847 * X_2 + 3.107 * X_3 + 0.420 * X_4 + 0.998 + X_5 \quad (2.16)$$

Розрахунок компонентів:

$$X_1 = \frac{\text{Оборотні активи} - \text{Поточні зобов}'\text{язання}}{\text{Загальні активи}} \quad (2.18)$$

$$X_1 = \frac{146{,}688 \text{ тис. грн} - 1{,}536 \text{ тис. грн}}{192{,}673 \text{ тис. грн}} = 0{,}753$$

$$X_2 = \frac{\text{Нерозподілений прибуток}}{\text{Загальні активи}} \quad (2.18)$$

Таблиця 2.2

Сформований SWOT-аналіз рівня економічної безпеки підприємства

Сильні сторони: 1. Різноманітний сортовий діапазон вирощуваної продукції 2. Значні площі земельних угідь 3. Висококваліфікований і досвідчений персонал 4. Доступ до сучасних технологій	*Слабкі сторони:* 1. Сезонна робота 2. Відсутність широкої мережі збуту 3. Висока залежність від погодних умов
Можливості: 1.Встановлення новітніх технологій для полегшення та автоматизації виробництва 2. Розширення ринків збуту 3.Ворощування нових сортів гібридів	*Загрози:* 1. Зростання конкуренції на ринку 2. Несприятливі погодні умови 3. Військові дії 3. Зміни в законодавстві 4. Коливання цін які змінюють собівартість виробництва

$$X_2 = \frac{187{,}309 \text{ тис. грн}}{192{,}673 \text{ тис. грн}} = 0{,}972$$

$$X_3 = \frac{\text{Операційний прибуток}}{\text{Загальні активи}} \quad (2.19)$$

$$X_3 = \frac{3{,}201 \text{ тис. грн}}{192{,}673 \text{ тис. грн}} = 0{,}017$$

$$X_4 = \frac{\text{Власний капітал}}{\text{Загальні зобов′язання}} \quad (2.20)$$

$$X_4 = \frac{191{,}137 \text{ тис. грн}}{1{,}536 \text{ тис. грн}} = 124{,}48$$

$$X_5 = \frac{\text{Дохід від продажу}}{\text{Загальні активи}} \quad (2.21)$$

$$X_5 = \frac{88{,}294 \text{ тис. грн}}{192{,}673 \text{ тис. грн}} = 0{,}458$$

Підставляємо отримані значення у формулу (2.16):

$$Z = 0.717 \times 0.753 + 0.847 \times 0.972 + 3.107 \times 0.017 + 0.420 \times 124.48 + 0.998 \times 0.458 = 0.540 + 0.823 + 0.053 + 52.281 + 0.457 = 54.154$$

Отже, за розрахунками показника Альтмана, ТОВ Агрофірма «Славутич» має показник 54,154. Це значення свідчить про те, що товариство має високу фінансову стійкість та низьку ймовірність банкрутства.

2.3. Дослідження поточного захисту комерційної таємниці та вразливих даних у ТОВ Агрофірма «Славутич»

У цьому розділі здійснено оцінку ефективності заходів із захисту КТ в ТОВ «Славутич», яке функціонує в сфері сільськогосподарського виробництва. Метою дослідження є визначення рівня ефективності реалізованих заходів захисту інформації, виявлення існуючих загроз і вразливостей, а також пошук можливостей для вдосконалення цих процесів.

Першим етапом стало аналізування поточного стану системи управління КТ. У рамках цього етапу було проведено порівняння існуючих політик, процедур та технічних засобів захисту з міжнародними стандартами та найкращими практиками у сфері захисту комерційної інформації та кібербезпеки. Основні стандарти для оцінки включали ISO 27001

(міжнародний стандарт, що встановлює вимоги до систем управління інформаційною безпекою), NIST Cybersecurity Framework (фреймворк кібербезпеки від Національного інституту стандартів і технологій США), CIS Controls (рекомендації з кібербезпеки від Центру кібербезпеки) та GDPR (Загальний регламент захисту даних Європейського Союзу) [1].

Аналіз показав, що система управління КТ у ТОВ «Славутич» в цілому відповідає стандартам на середньому рівні. Виявлено, що існуючі політики та процедури з захисту інформації лише частково узгоджуються з вимогами ISO 27001, а також спостерігаються прогалини у дотриманні рекомендацій NIST Cybersecurity Framework і CIS Controls.

Основним фактором невідповідності стандарту ISO 27001 є неповна і нечітка документація політик і процедур, а також недостатня увага до реалізації та перевірки ефективності контрольних заходів. Стандарт ISO 27001 визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням потенційних загроз і вимог зацікавлених сторін [1].

Враховуючи зазначене, для ТОВ «Славутич» є критично важливим ретельно переглянути та оновити свої політики і процедури захисту інформації, забезпечивши їх відповідність встановленим вимогам, а також впровадити ефективні механізми їх реалізації та дотримання всіма співробітниками компанії. Крім того, необхідно створити систему постійного моніторингу та оцінки виконання вимог стандарту ISO 27001 для підтримки безперервного вдосконалення системи управління комерційною таємницею.

Щодо NIST Cybersecurity Framework, було виявлено окремі недоліки у впровадженні необхідних контролів. Зокрема, недостатньо або неналежно реалізовано контроль доступу до конфіденційної інформації. Також виявлено відсутність повноцінного моніторингу та аналізу подій, що є важливими компонентами цього фреймворку.

Аналіз впровадження рекомендацій CIS Controls показав, що деякі необхідні заходи не були належно інтегровані через брак відповідних технічних рішень або процедур. Зокрема, контроль за виявленням і реагуванням на інциденти залишався недостатньо розробленим, що може спричинити затримки у реагуванні на потенційні загрози. Отже, система управління комерційною таємницею потребує подальшого вдосконалення.

Проведене порівняння дозволило оцінити поточний рівень відповідності наявних заходів у сфері кібербезпеки, виявити існуючі прогалини та сформулювати напрями для покращення системи управління комерційною таємницею.

Наступним кроком було проведення аналізу загроз та вразливостей які були ідентифіковані. Основна увага була приділена можливим технічним атакам, ризикам соціальної інженерії та внутрішнім загрозам, що можуть виходити від співробітників.

Стосовно технічних атак, дослідження вказало на потенційні ризики, пов'язані з використанням застарілих програмних рішень та існуючими вразливостями в мережевій інфраструктурі компанії. Аналізувалися ймовірність атак, здійснюваних через шкідливе програмне забезпечення та методи злому, які можуть призвести до несанкціонованого доступу до конфіденційних даних і компрометації безпеки.

Щодо соціальної інженерії, дослідження було спрямоване на вивчення сценаріїв, де зловмисники могли б використовувати маніпуляцію працівниками для отримання неправомірних доступів до конфіденційної інформації.

Виявлено також можливі внутрішні загрози, які можуть спричинити витік інформації або несанкціонований доступ до даних з боку співробітників. Це може бути пов’язано з недостатньою професійною підготовкою персоналу або недотриманням ними процедур безпеки.

Результати дослідження вказують на наявність ризиків за всіма цими напрямками та підкреслюють важливість впровадження заходів для зниження вразливостей і зміцнення захисту інформації в ТОВ «Славутич». До таких заходів можуть належати підвищення обізнаності співробітників з питань кібербезпеки, встановлення систем моніторингу та виявлення загроз, а також посилення технічних засобів захисту мережевої та інформаційної інфраструктури.

Наступним кроком була проведена оцінка заходів захисту які існують у товаристві. Аналіз включав перевірку того, наскільки успішно існуючі заходи запобігають потенційним атакам і як ефективно вони реагують на актуальні загрози.

Детальне дослідження показало, що система захисту в ТОВ «Славутич» має свої сильні сторони, але також потребує вдосконалення для належного захисту від ідентифікованих загроз. З огляду на виявлені ризики, стало зрозуміло, що наявні технічні засоби, такі як мережеві файрволи, антивірусне програмне забезпечення та системи виявлення вторгнень, потребують оновлення до сучасніших версій. Деякі слабкі місця було виявлено у процесах виявлення певних типів загроз, зокрема, тих, що виникають внаслідок дій працівників, що призводить до затримок у реагуванні.

Щодо механізмів реагування на атаки чи порушення безпеки, які включають процедури аналізу та відновлення системи, вони показали достатній рівень ефективності. Однак є певні аспекти, де можна підвищити швидкість виявлення та ізоляції загроз, що сприятиме більш оперативній реакції. Головні загрози захисту КТ на підприємстві зображені на рисунку 2.11.

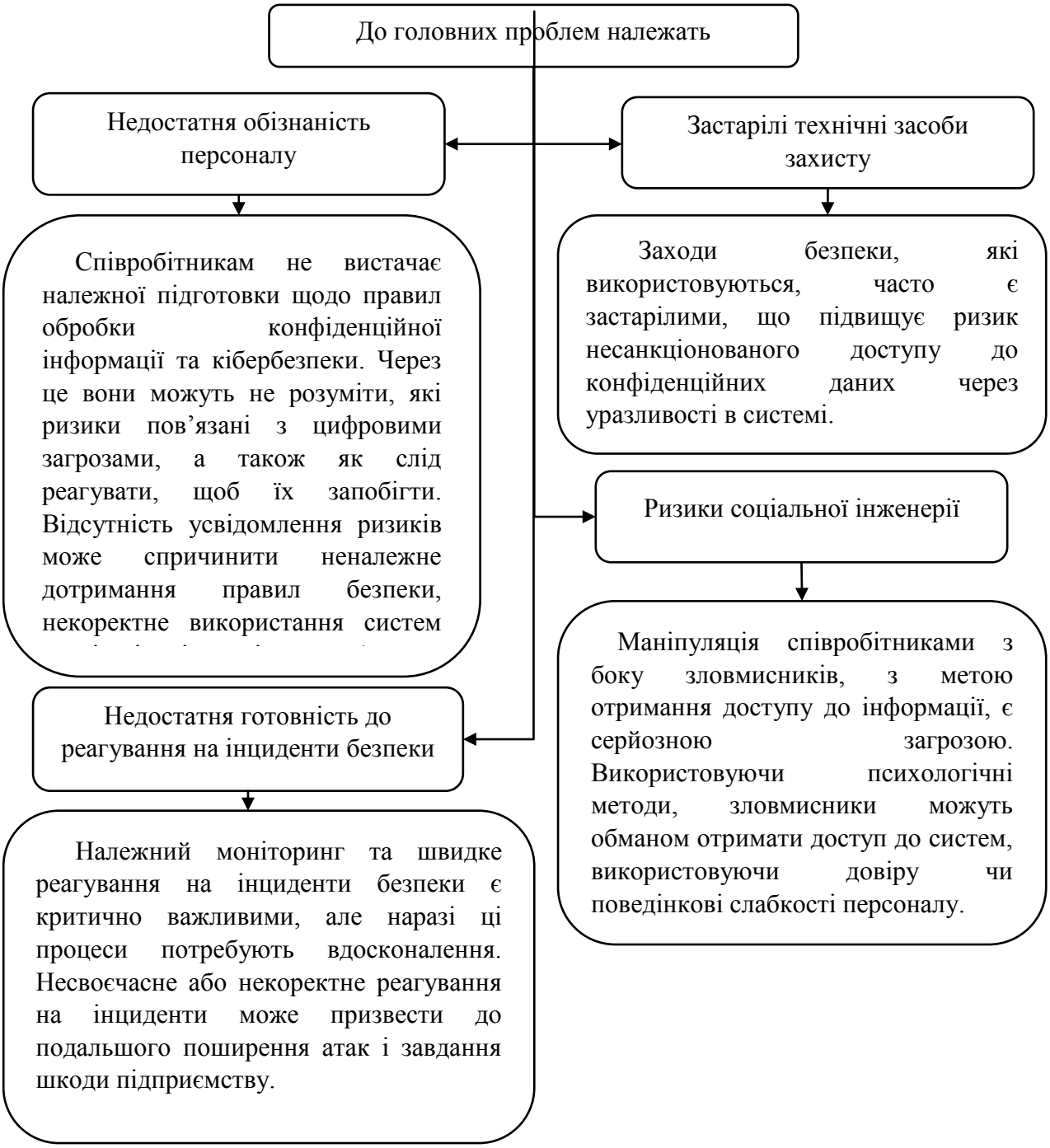

Рис. 2.11. Схема виявлених загроз захисту в ТОВ Агрофірма «Славутич»

Процедурні заходи, такі як політики доступу до інформації та процедури аутентифікації, продемонстрували свою ефективність. Водночас є можливість для вдосконалення, особливо у сфері моніторингу та аналізу активності користувачів з метою виявлення підозрілих або аномальних дій.

Існуючі проблеми на підприємстві стосуються як технічних, так і організаційних аспектів діяльності. До організаційних аспектів належать недостатньо розроблені політики та процедури, низький рівень обізнаності

персоналу в питаннях кібербезпеки, а також недоліки в управлінні ризиками та реагуванні на інциденти. З технічного боку, виявлено вразливості в програмному забезпеченні та інфраструктурі, відсутність належного шифрування та ідентифікації, а також обмежену ефективність захисних засобів, як-от брандмауери й антивірусні програми. У зв'язку з цим, необхідно детально проаналізувати кожну з цих проблем, щоб створити комплексний план захисту комерційної таємниці.

На основі результатів оцінки розроблено рекомендації для підвищення рівня захисту, оновлення політик і процедур, а також покращення знань персоналу в сфері кібербезпеки.

Одним із пріоритетів є підвищення обізнаності працівників щодо кібербезпеки та принципів управління комерційною таємницею. Пропонується організувати серію навчальних заходів, таких як семінари, тренінги або вебінари з кібербезпеки та правильного поводження з конфіденційною інформацією. Це сприятиме кращому розумінню персоналом потенційних загроз і необхідних заходів захисту.

Наступний пріоритет — оновлення технічних засобів захисту. Рекомендується оновити програмне забезпечення до останніх версій, що містять виправлені вразливості, а також впровадити сучасні механізми моніторингу безпеки і новітні антивірусні системи. Ще один пріоритет полягає у вдосконаленні політик і процедур, пов’язаних із комерційною таємницею. Сюди входить розробка чітких правил доступу до конфіденційної інформації, запровадження процедур контролю за змінами та регулярний перегляд політик з урахуванням нових загроз і змін у законодавстві.

Останнім важливим пріоритетом є покращення системи моніторингу та реагування на інциденти безпеки. Впровадження автоматизованих систем виявлення порушень безпеки, посилення механізмів моніторингу та аналізу

подій, а також створення швидких і ефективних процедур реагування на загрози.

Висновки до другого розділу

1. ТОВ Агрофірма «Славутич» здійснює свою діяльність у сфері сільськогосподарського виробництва протягом багатьох років, орієнтуючись на вирощування зернових, бобових і олійних культур. Аналіз фінансово-економічної діяльності підприємства показав як позитивні тенденції, такі як зростання вартості необоротних активів, так і певні проблеми, зокрема зношення основних засобів та нестабільність чистого доходу. Загалом ситуація на підприємстві контрольована, хоча потребує вдосконалення для забезпечення стабільного розвитку.

2. Для обробки інформації та звітності компанія активно використовує сучасне програмне забезпечення, що дозволяє автоматизувати облік і підвищити ефективність операцій. Проте на підприємстві відсутній окремий відділ економічної безпеки, а відповідальність за її забезпечення покладена на керівників структурних підрозділів, зокрема бухгалтерську службу під керівництвом головного бухгалтера.

3. Оцінка рівнів економічної безпеки показала, що правова, екологічна та кадрова складові перебувають на достатньому рівні. Водночас виявлено відхилення у технологічній, інформаційній, інтелектуальній та силовій складових. Зокрема, фінансова складова є занадто низькою для стабільного функціонування підприємства, що вимагає особливої уваги до цього аспекту.

4. Діагностика технічного стану основних засобів показала їхнє значне зношення, що може негативно вплинути на ефективність виробничих процесів. Відсутність оновлення технічного парку підприємства призводить

до збільшення витрат на обслуговування і може створити ризики для подальшого зростання.

5. Аналіз оборотності активів виявив зниження ефективності їх використання, що свідчить про проблеми з ліквідністю та підвищене операційне навантаження. Незважаючи на це, підприємство демонструє адаптивність до ринкових викликів і здатність відновлювати доходи, хоча потрібна оптимізація фінансових ресурсів та підвищення контролю за витратами.

6. Для забезпечення стабільної роботи підприємства рекомендовано створити окремий відділ економічної безпеки, який би відповідав за моніторинг фінансових ризиків, захист інформації, кадрову безпеку та розробку антикризових заходів.

3. УДОСКОНАЛЕННЯ ЗАХИСТУ ВРАЗЛИВИХ ДАНИХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НА ПІДПРИЄМСТВІ ТОВ АГРОФІРМА «СЛАВУТИЧ»

3.1. Удосконалення системи інформаційної безпеки підприємства ТОВ Агрофірма «Славутич»

Інформаційна безпека сучасного підприємства знаходиться під постійним тиском загроз, які швидко розвиваються та змінюються. В умовах, коли цифрові технології стають основою більшості бізнес-процесів, підприємства стикаються з численними викликами, пов’язаними із забезпеченням конфіденційності, цілісності та доступності інформації. Для ТОВ Агрофірма «Славутич», як і для багатьох інших компаній, ці виклики є особливо актуальними.

Однією з ключових загроз є фішингові атаки. Вони полягають у використанні підроблених електронних листів або веб-ресурсів для введення в оману співробітників підприємства з метою отримання конфіденційних даних. Це може бути інформація про доступ до внутрішніх систем, фінансові операції або навіть особисті дані співробітників. Для аграрного сектора, де часто використовуються автоматизовані системи управління, втрата такої інформації може призвести до збоїв у ланцюжках поставок і суттєвих фінансових збитків.

Ще однією небезпекою є внутрішні загрози, зокрема дії або недбалість співробітників, які мають доступ до критично важливих даних. Наявність необізнаного або зловмисного персоналу може створювати суттєві ризики. Наприклад, ненавмисне використання незахищених пристроїв, нехтування правилами збереження паролів або передача конфіденційних даних третім особам можуть стати причиною витоків інформації.

Застаріла інфраструктура захисту даних також становить значний ризик. Багато підприємств використовують традиційні методи захисту, які вже не відповідають сучасним викликам. Наприклад, паролі, які не оновлюються регулярно, або відсутність шифрування даних під час їх передачі, відкривають можливості для зловмисників. У випадку ТОВ Агрофірма «Славутич» це може вплинути на безпеку систем, що забезпечують управління земельними ресурсами, фінансами чи договорами.

Важливим викликом є також соціальна інженерія. Це методика, яка базується на маніпуляції людьми з метою отримання доступу до конфіденційної інформації. Зловмисники можуть, наприклад, представлятися керівниками підприємства або важливими клієнтами, щоб отримати дані про фінансові операції. Враховуючи специфіку аграрного сектора, де значна частина комунікації з партнерами відбувається дистанційно, ризики соціальної інженерії є досить високими.

Не можна ігнорувати й кібератаки на виробничу інфраструктуру, особливо в контексті використання автоматизованих систем управління аграрними процесами. Такі атаки можуть бути спрямовані на порушення роботи обладнання, крадіжку технологічних секретів або маніпуляції з даними, що використовуються для планування виробництва. Наприклад, викривлення інформації про погодні умови, використання ресурсів або посівні площі може призвести до значних втрат.

Серед інших викликів — регуляторні ризики. Зростаюча кількість нормативно-правових актів, які регулюють захист даних (наприклад, GDPR у Європейському Союзі), зобов’язує підприємства впроваджувати відповідні засоби захисту та звітувати про інциденти безпеки. Недотримання таких вимог може призвести до штрафів та втрати репутації.

Таким чином, ТОВ Агрофірма «Славутич» стикається з багатогранними загрозами для інформаційної безпеки. Ефективна протидія цим викликам вимагає комплексного підходу, що включає не лише

впровадження сучасних технологій, але й підвищення обізнаності співробітників, удосконалення політик управління ризиками та адаптацію до динамічних умов сучасного кіберпростору.

Які загрози несуть фішингові повідомлення та з якою метою їх використовують зловмисники. Насамперед такі атаки завдають значної шкоди як особистої для працівника так і для компанії, їхньою особливістю стає те що вони таким чином здатні обходити технічні заходи захисту, спираючись на людський фактор. Для нашого підприємства це також маже мати наслідки.

Зловмисники можуть задіяти від імені компанії масштабовану персоналізацію атак використовуючи дані про підприємство. Імітуючи комунікацію від імені нових або постійних постачальників, клієнтів чи державних органів. Як варіант виконуюча особа може отримати повідомлення від так званого «нового постачальника», яке буде містити небезпечне посилання чи вкладення. Схожість з попередніми виконаними завданнями підвищує шанси на відкриття повідомлення. Також такі атаки та посилання розповсюджені у популярних соціальних платформах таких як Viber, Telegram та WhatsApp. Зазвичай такі листи виглядають як комерційна пропозиція або інформація про вигідну акцію від компанії партнера, або інформація з новим каталогом асортименту продукції, послуг чи товарів. У таких випадках співробітники ризикують передати шахраям доступ до свої пристроїв.

До типових сценаріїв з фішинговими повідомленнями відносяться наступні ситуації. Повідомлення від «Нових постачальників» в яких шахраї, представляються потенційними партнерами. У свої листах вони пишуть про пропозиції на вигідних умовах до співпраці, презентації нових продуктів та інше. Такий лист виглядає як текстове повідомлення з вкладеним матеріалом формату PDF чи Excel, а посилання має вигляд як доступ до онлайн каталогу.

Також такі атаки часто мають схожість на «Запити про оплату». Такі листи імітують рахунки або платіжні вимоги від імені існуючих партнерів компанії. За такого сценарію виникає небезпека переказу коштів на рахунки зловмисників.

Ще як варіант такі листи приходять як повідомлення про безпеку особистого аккаунту. Зазвичай вони імітують листи від центру сповіщень програмного забезпечення, та містять інформацію про необхідність підтвердження особистих даних та електронної пошти, також можуть мати текст з проханням оновити пароль.

Через месенджери, зловмисники здатні надсилати повідомлення від колег або керівництва з проханням передати дані для входу до корпоративних облікових записів.

Які небезпеки від описаних повідомлень та які наді бажають викрасти шахраї. Якщо співробітник переходить за фішинговим повідомленням та завантажує небезпечні вкладення в них з’являється вірогідність витоку таких даних:

- Дані для доступу до корпоративних облікових записів (логіни, паролі, двофакторні коди);
- Фінансову інформацію (номери рахунків, дані про трансакції);
- Комерційні секрети (договірні умови, ціни, технологічні процеси);
- Персональні дані співробітників (адреси, номери телефонів, ідентифікаційні коди).

Через месенджери, наприклад, WhatsApp або Telegram, шахраї можуть отримувати файли із внутрішньою інформацією або здійснювати атаки за допомогою фішингових посилань надсилаючи їх до людей з облікової книжки спілкування. Через відкриття такого повідомлення на телефоні може призвести до компрометації пристрою та подальшого витоку інформації через встановлення шпигунського ПЗ. На рисунку 3.1 описані небезпеки для корпоративної пошти.

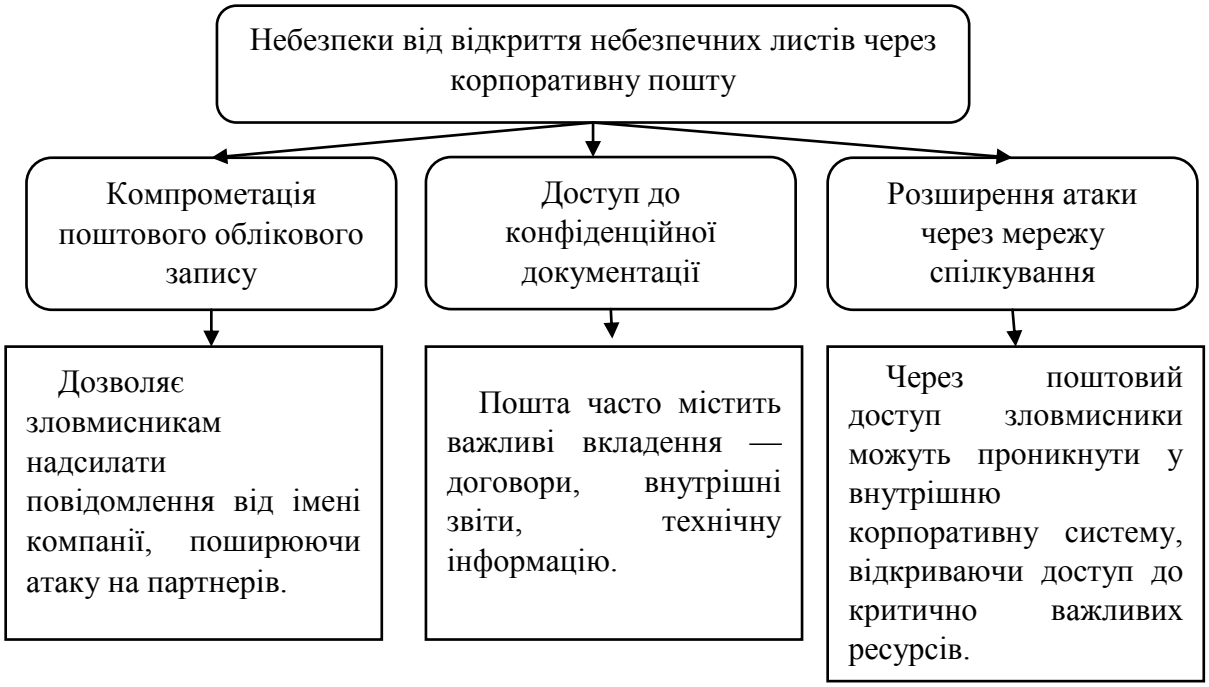

Рис. 3.1. Побудований інформаційний масив небезпек впливу на ТОВ Агрофірма «Славутич» від фішингових атак на корпоративну пошту підприємства

Тож підсумовуючи, фішингові атаки становлять багатогранну загрозу для інформаційної безпеки ТОВ Агрофірма «Славутич». Їхній вплив може бути відчутним: від фінансових втрат до зупинки виробничих процесів. Для зменшення ризиків важливо запроваджувати сучасні технології захисту, регулярно проводити тренінги для співробітників та дотримуватися суворих політик безпеки при використанні як корпоративних, так і персональних пристроїв.

3.2. Розробка концепції програмного забезпечення SkamBlock для ТОВ Агрофірма «Славутич» з метою протидії фішинговим атакам із застосуванням сучасних методів шифрування

Фішингові атаки є однією з найбільш поширених форм кіберзагроз, що спрямовані на викрадення конфіденційної інформації, облікових даних і

фінансових ресурсів підприємств. У відповідь на цю проблему було розроблено інноваційну концепцію системи захисту, яка поєднує передові технології автоматизованого аналізу повідомлень, адаптивні алгоритми машинного навчання та сучасні методи шифрування даних.

Основні компоненти системи захисту

1. Інтеграція з корпоративними інформаційними системами Система впроваджується безпосередньо в інформаційну інфраструктуру підприємства, інтегруючись із поштовими серверами, базами даних та системами управління бізнес-процесами. Це дозволяє забезпечити всебічний моніторинг електронної комунікації, оперативно виявляючи потенційно небезпечні повідомлення.

2. Аналіз вхідних повідомлень за допомогою програмних алгоритмів. На рисунку 3.2. зображено що кожен електронний лист проходить багаторівневу перевірку:

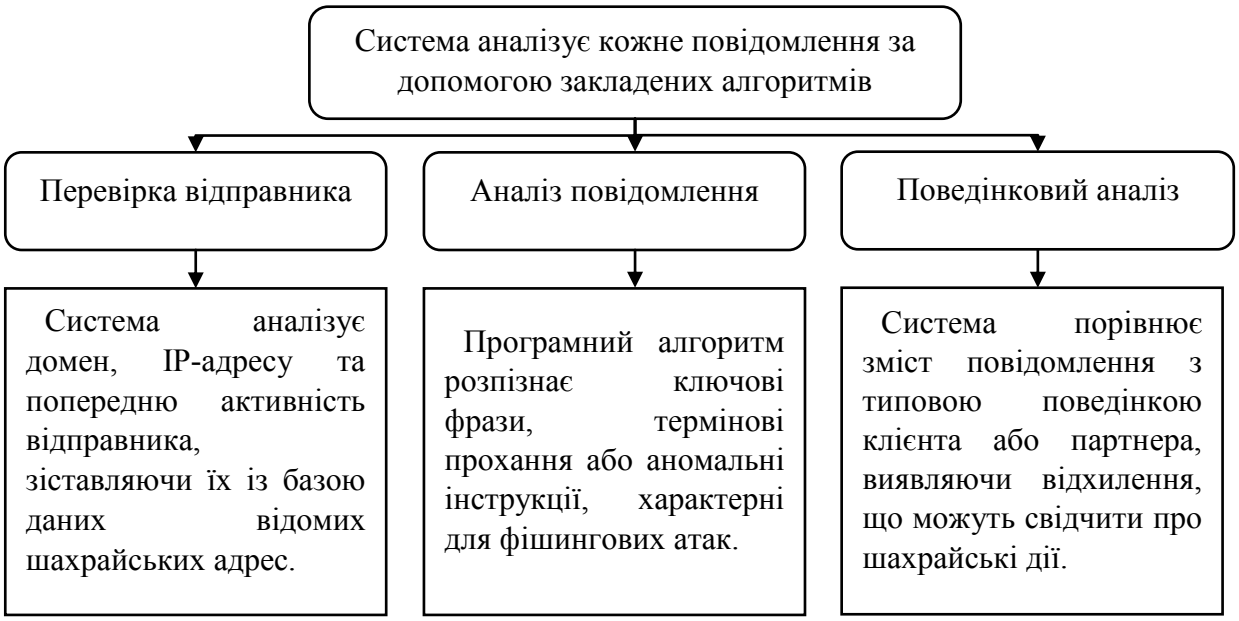

Рис. 3.2. Запропонована система аналізу повідомлень за для дотримання безпеки листування на підприємстві ТОВ Агрофірма «Славутич»

3. Механізми навчання на основі реальних інцидентів Алгоритми машинного навчання постійно оновлюються на основі нових

випадків атак, які виявляються в системі. Забезпечує адаптацію до змінних методів, які використовують кіберзлочинці, дозволяючи системі ідентифікувати навіть раніше невідомі загрози.

4. Використання сучасних методів шифрування

Значна увага у розробці системи приділяється захисту даних на всіх етапах їх обробки та передачі. Для цього використовуються передові методи шифрування, які забезпечують як конфіденційність, так і цілісність інформації:

- Технологія гомоморфного шифрування дозволяє виконувати операції над зашифрованими даними без необхідності їх розшифровки. Завдяки цьому система аналізує вміст електронних листів, залишаючи їх у зашифрованому вигляді, що мінімізує ризик витоку даних навіть у разі компрометації системи. Гомоморфне шифрування гарантує, що вся обробка даних відбувається під надійним захистом.
- Для забезпечення безпеки передачі ключів між компонентами системи використовується асиметричне шифрування технології RSA або ECC (еліптичні криві). Так зменшується ймовірність перехоплення ключів, які використовуються для шифрування й дешифрування даних.
- Поєднання гомоморфного та симетричного шифрування. Дані передаються у симетрично зашифрованому вигляді, але ключі для шифрування захищені за допомогою асиметричного алгоритму. Гібридний підхід забезпечує оптимальне поєднання високої продуктивності та максимального рівня захисту.

Протидія фальшивим транзакціям

Особливу увагу в системі приділено фінансовій безпеці. Усі запити на зміну фінансових реквізитів або виконання транзакцій, що надходять через електронну пошту, проходять додаткову перевірку:

- Виявлення аномалій у фінансових даних.
- Контроль відповідності запиту попередній взаємодії з клієнтом.

- Залучення багатофакторної автентифікації для підтвердження критичних дій.

Очікувані результати впровадження

Розроблена система дозволить ТОВ Агрофірма «Славутич»:

- Скоротити кількість успішних фішингових атак, запобігаючи втратам даних і фінансів.
- Підвищити довіру партнерів і клієнтів завдяки впровадженню сучасних методів захисту.
- Забезпечити відповідність міжнародним стандартам інформаційної безпеки.
- Оптимізувати процеси виявлення та реагування на загрози, зменшивши час реакції до кількох секунд. Основні системні дії, які має виконувати розроблена система зображено на рисунку 3.3.

Рис. 3.3. Розроблені основні системні дії, які має виконувати система виявлення та запобігання фішингових атак SkamBlock

Запропонована концепція комплексного захисту від фішингових атак із використанням гомоморфного шифрування, адаптивних алгоритмів аналізу даних і асиметричних методів шифрування створює новий рівень інформаційної безпеки. Впровадження забезпечить надійний захист критично важливих даних, мінімізуючи ризики та зміцнюючи позиції ТОВ Агрофірма «Славутич» у конкурентному середовищі.

Наступним кроком складаю вимоги роботи програмного забезпечення що аналізує електронні листи компанії, але зберігає їхній вміст у зашифрованому вигляді та гарантує конфіденційність даних.

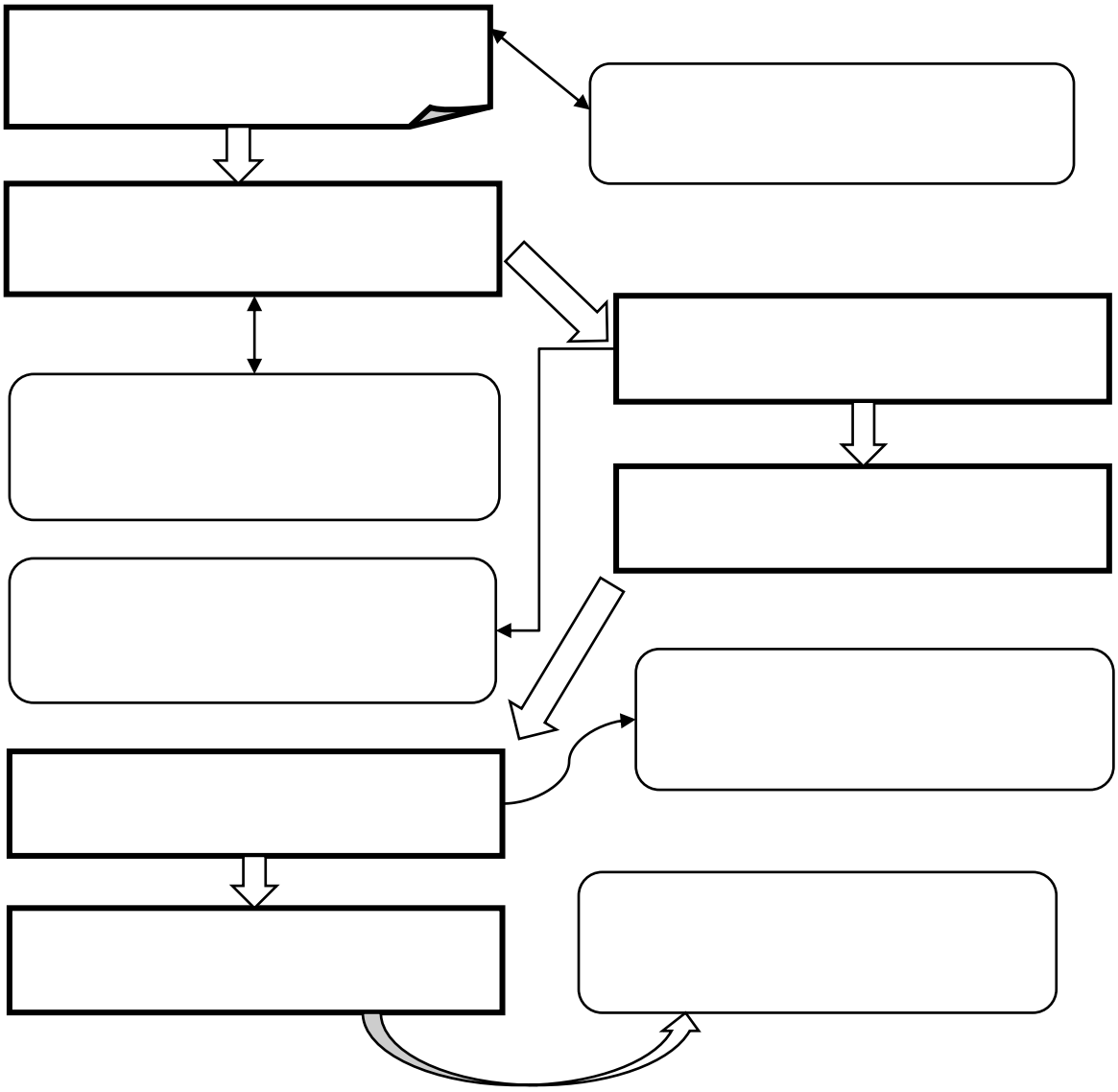

Рис.3.4 Розроблений процес аналізу вхідного ПЗ SkamBlock, як механізм захисту КТ підприємства від фішингових повідомлень

Для доступу до поштових серверів компанії програмне забезпечення буде здійснювати підключення за IMAP/SMTP, буде читати тільки ті листи на які електронні пошти налаштована програма, всі листи при обробці залишаються у зашифрованому вигляді.

Для обробки даних у зашифрованому вигляді буде використовуватися гомоморфне шифрування, саме воно має властивість обробляти інформацію у зашифрованому вигляді.

Щоб гарантувати безпеку та уникнути витоку інформації програмне забезпечення буде працювати в ізольованому середовищі такому як сервер з обмеженим доступом. Асиметричне шифрування буде використовуватися для передачі ключів (RSA/ECC), а для роботи з листами симетричне (AES).

1. Інтеграція з поштовою системою здійснюється через IMAP. Використовуючи підключення до поштового сервера з використанням облікових даних які зберігаються у зашифрованому вигляді.

Листи зберігаються в зашифрованому вигляді навіть на етапі обробки.

2. Щоб забезпечити гомоморфне шифрування інтегруємо роботу з Microsoft SEAL:

SEAL забезпечить підтримку шифрування числових даних (частот слів у тексті), це дозволить проводити складний аналіз.

3. Гібридне шифрування комбінує швидке симетричне шифрування (для даних) і надійне асиметричне (для передачі ключів).

Ключ AES використовується для шифрування листа. Ключ AES сам передається в зашифрованому вигляді через RSA.

4. Аналіз зашифрованих листів

Машинне навчання буде адаптовано до зашифрованих даних, через обчислення частот ключових слів.

5. Безпечна архітектура

Програма працює в ізольованому середовищі Docker:

Серверні обмеження - Обмежуємо доступ до контейнера через VPN. Віддалений доступ лише для адміністратора через SSH із двофакторною аутентифікацією.

Переваги системи:

1. Всі листи зберігаються та аналізуються в зашифрованому вигляді.

2. Результати аналізу доступні лише уповноваженим системам.

3. Ізольоване ядро гарантує, що ніхто не отримає доступ до листів у разі спроб злому доступу до програмного забезпечення. Розроблений механізм нового програмного забезпечення SkamBlock який буде протидіяти фішинговим атакам на підприємстві представлений у додатку А.

3.3. Розрахунок економічної ефективності впровадження розробленого ПЗ в ТОВ Агрофірма «Славутич»

Далі проведемо розрахунок впровадження розробки та окупності запропонованого ПЗ. ТОВ Агрофірма «Славутич», яка налічує 73 співробітників, із них 30 мають доступ до конфіденційної інформації, повинна забезпечити ефективний захист даних. Мій аналіз доводить, що впровадження захисного програмного забезпечення є не лише доцільним, а й економічно вигідним, враховуючи можливі втрати від атак та перспективи збільшення доходу.

Уникненні фінансові втрати: оцінка ризиків та економічний ефект. Для оцінки уникненні фінансових втрат я застосував формулу:

$$\text{Втун} = (\text{Кбез} - \text{Кз}) \times \text{Ватаки} \quad (3.1)$$

Де:

$В_{тун}$ — уникненні фінансові втрати, грн;

$К_{без}$ — кількість атак без ПЗ, шт;

$К_{з}$ — кількість атак із ПЗ, шт;

$В_{атаки}$ — вартість ліквідації наслідків однієї атаки, грн.

Для $К_{без}$ згідно з практикою у сфері кібербезпеки, близько 30% співробітників без ПЗ можуть стати жертвами фішингових атак. Я вважаю цей показник реалістичним, оскільки співробітники, що працюють із критичними даними, частіше зазнають спроб шахрайства. Водночас ефективність сучасного програмного забезпечення знижує ризик атак на 80%:

$$Кбез = 30 \times 0.3 = 9 \text{ атак.}$$

Для $К_з$, з урахуванням ефективності ПЗ у 80%:

$$Кз = 9 \times (1 - 0.8) = 1.8 \text{ атак}$$

Середня вартість атаки в $1000 є типовою для компаній середнього розміру. Ця сума включає витрати на ліквідацію наслідків, компенсацію клієнтам і втрату продуктивності. У моїй практиці я бачив, як подібні інциденти ставали значним ударом для бюджету компаній.

Розрахуємо $В_{тун}$:

$$Втун = (9 - 1.8) \times 41{,}400 = 7.2 \times 41{,}400 = 298{,}080 \text{грн.}$$

2. Зростання доходу

Очікуване підвищення доходу я оцінював за формулою:

$$Ддод = Дбаз \times \%зрост \qquad (3.2)$$

Де:

$Д_{дод}$ — додатковий дохід, грн;

$Д_{баз}$ — базовий дохід компанії, грн;

$\%_{зрост}$ — відсоток зростання доходу.

Згідно з фінансовими даними за 2023 рік, $Д_{баз}$=79,930,000 , а приріст доходу оцінюється у $\%_{зрост}$ = 5%. Чому саме 5%.
На мою думку, цей показник є обґрунтованим, оскільки дослідження компанії Gartner вказують, що підвищення репутації та зниження кількості помилок працівників може забезпечити приріст доходу до 5%. Для ТОВ

«Славутич», де річний дохід становить 79,930,000 грн, це виглядає перспективно.

$$\text{Ддод} = 79{,}930{,}000 \times 0.05 = 3{,}996{,}500\text{грн.}$$

3.Витрати на впровадження ПЗ

Розробка захисного програмного забезпечення вимагає інвестицій. На мою думку, вартість у $20,000 (828,000 грн) є адекватною для створення інструмента, що відповідає потребам компанії. Щорічні витрати на підтримку ($5000) забезпечують регулярні оновлення та технічну підтримку.

Формула:

$$\text{Впз} = \text{Врозр} + \text{Вобсл} \qquad (3.3)$$

Де:

$В_{пз}$ — загальна вартість ПЗ, грн;

$В_{розр}$ — вартість розробки ПЗ, грн;

$В_{обсл}$ — вартість щорічного обслуговування, грн.

Розрахунок:

$В_{розр}$ = 828,000грн, $В_{обсл}$ = 207,000 грн.

$$\text{Впз} = 828{,}000 + 207{,}000 = 1{,}035{,}000\text{грн.}$$

Графічне відображення процесу впровадження ПЗ для захисту КТ господарства представлено на рисунку 3.6.

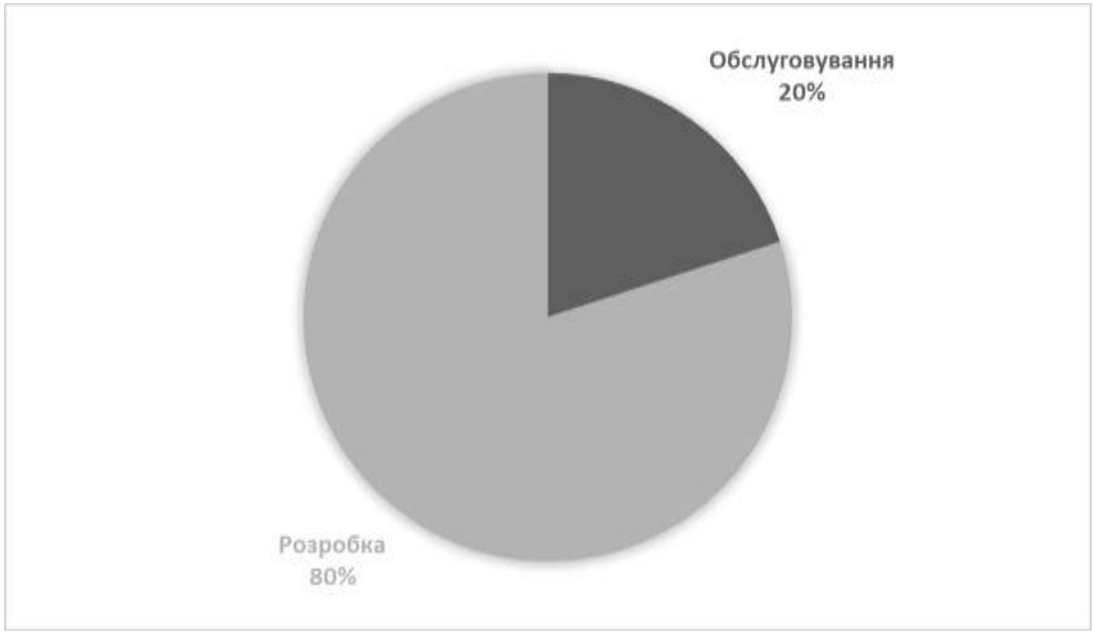

Рис. 3.6. Витрати на впровадження розробленого програмного забезпечення для ТОВ Агрофірма «Славутич»

4.Термін окупності:

Формула:

$$\text{Токуп} = \frac{\text{Впз}}{\text{Ерічн}} \quad (3.4)$$

Де:

$T_{окуп}$ — термін окупності, років;

$B_{пз}$ — загальна вартість ПЗ, грн;

$E_{річн}$ — річний економічний ефект, грн.

Розрахунок:

$$\text{Токуп} = \frac{1035000}{298080} = 3{,}47 \text{ роки}$$

Графік терміну окупності ПЗ SkamBlock зображено на рисунку 3.7.

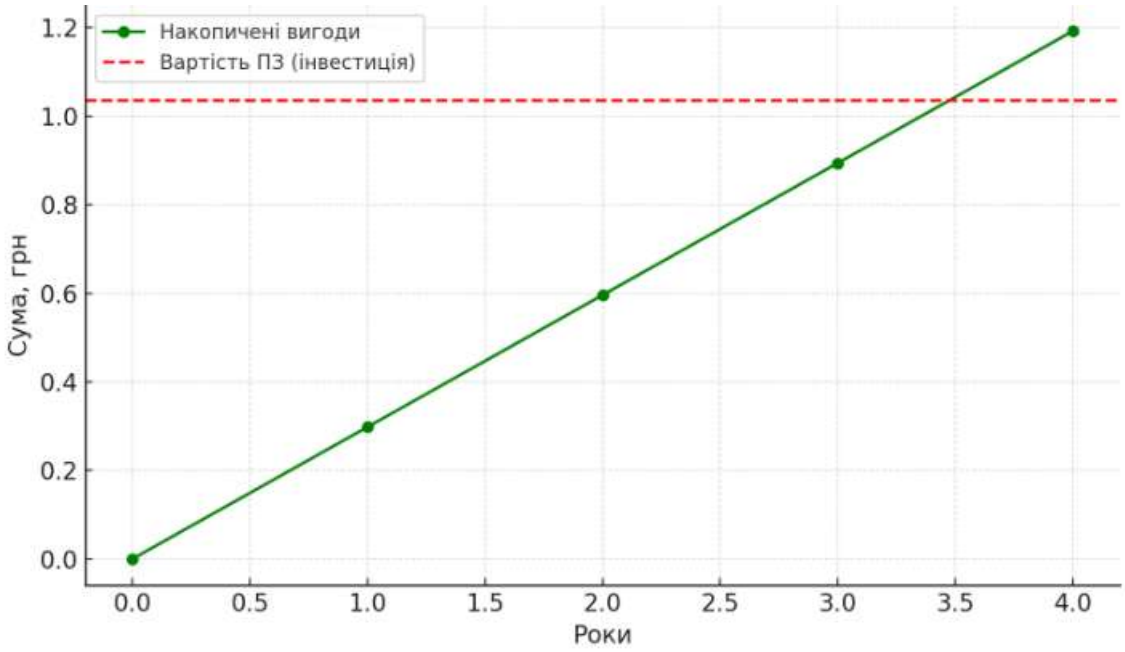

Рис. 3.7. Сформований графік терміну окупності ПЗ SkamBlock для підприємтсва

Це свідчить, що інвестиції окупляться за менш ніж 4 роки, що є вигідним для підприємства. На таблиці 3.1 наведені результати розрахунків.

Таблиця 3.1

Результати розрахунків впровадження ПЗ SkamBlock на ТОВ Агрофірма «Славутич»

Показник	USD	UAN (курс 41,40)
Уникненні втрати від атак	7200	298,080
Додатковий дохід	96,533	3,996,500
Вартість розробки ПЗ	20,000	828,000
Щорічне обслуговування ПЗ	5000	207,000
Загальна вартість ПЗ	25,000	1,035,000
Термін окупності (років)	3,47	3,47

Мої розрахунки показують, що впровадження програмного забезпечення для захисту від фішингових атак є економічно обґрунтованим. Окрім уникнення втрат у 298,080 грн щорічно, компанія отримає приріст доходу до 3,996,500 грн. При цьому програмне забезпечення окупиться за 3,47 року, що є значним аргументом на користь інвестицій.

Висновки до третього розділу

1. У цьому розділі я акцентую увагу на важливості комплексного підходу до захисту інформації яка є важливим ключовим ресурсом підприємства. Саме тому щоб забезпечити збереження конкурентних переваг, попередити фінансові збитки та зберегти довіру клієнтів необхідно подбати про ефективний захист інформації.

2. Запропонував широкий спектр заходів для захисту комерційної інформації, з використанням гомоморфного шифрування, яке дозволяє

обробляти дані у зашифрованому вигляді, та асиметричні методи захисту ключів (RSA, ECC). Підхід з використанням гібридного шифрування матиме високу продуктивність та надійність захисту навіть якщо хтось намагатиметься отримати доступ до окремих компонентів системи.

3. У розділі особливу увагу приділено системам моніторингу та запобіганню загрозам таким як фішингові атаки. Запропонував впровадження автоматизованих рішень для аналізу поведінкових аномалій у повідомленнях, додаткової перевірки фінансових транзакцій і двофакторної автентифікації.

4. Аналіз поточних політик і процедур ТОВ Агрофірма «Славутич» показав, що система управління комерційною таємницею частково відповідає вимогам міжнародних стандартів ISO 27001, NIST Cybersecurity Framework і GDPR. Основними недоліками є нечіткість документації та недостатня реалізація контрольних заходів, що знижує загальний рівень інформаційної безпеки.

5. Запропоновано впровадження системи постійного моніторингу, оновлення програмного забезпечення та посилення заходів реагування на дії зловмисників.

6. У розгляді цього пункту запропонував оновити технічні засоби безпеки, впровадити сучасні антивірусні програми, посилити навчання персоналу та інтегрувати нові методи оцінки ризиків.

7. За очікуваними результатами впровадження рішень які запропоновано, значно вдасться зменшити обсяг успішних фішингових атак та підвищити інформаційну безпеку на товаристві. А також розроблене програмне забезпечення дозволить зменшити час на навчання персоналу та їх перевірку, так як буде виконувати аналіз та перевірку листів самостійно що також дозволить знизити людський фактор у витоку даних.

ВИСНОВКИ

1. ТОВ Агрофірма «Славутич» здійснює діяльність у сільськогосподарському секторі з акцентом на вирощуванні зернових, бобових і олійних культур. Підприємство демонструє стійкі результати в умовах сучасного ринкового середовища, проте аналіз виявив низку факторів, які впливають на рівень економічної безпеки. Зокрема, значне зношення основних засобів, нестабільність фінансових показників і відсутність централізованої системи управління економічною безпекою створюють ризики для подальшого зростання. Водночас підприємство зберігає контроль над основними показниками, що свідчить про його адаптивність і потенціал до покращення.

2. Підприємство активно використовує сучасне програмне забезпечення для ведення бухгалтерського обліку та подачі звітності. Зокрема, застосування автоматизованих систем дозволяє знизити ризики помилок, підвищити точність облікових даних і спростити процеси податкового адміністрування. Однак відсутність спеціалізованого відділу економічної безпеки обмежує ефективність управління ризиками та захисту інформаційних ресурсів.

3. Аналіз ключових складових економічної безпеки підприємства показав, що правова, екологічна та кадрова компоненти знаходяться на задовільному рівні. Натомість інформаційна, технологічна, фінансова та інтелектуальна складові потребують значного вдосконалення. Зокрема, фінансова складова характеризується низьким рівнем стабільності через залежність від позикових коштів та нестабільний дохід. Інтелектуальна складова обмежена недостатньою увагою до інновацій і патентного захисту.

4. Зношеність основних засобів підприємства досягла критичного рівня, що негативно впливає на ефективність виробничих процесів. Оновлення та модернізація технічного парку є пріоритетним завданням для

підвищення продуктивності, зменшення витрат на ремонт та забезпечення довгострокової конкурентоспроможності.

5. Сучасні виклики, такі як кіберзагрози, фішингові атаки, недоліки в управлінні доступом і людський фактор, вимагають впровадження багаторівневої системи захисту інформації. Відсутність систематичного підходу до ідентифікації та оцінки ризиків може призвести до фінансових втрат і витоку конфіденційної інформації.

6. Запропоновано створити спеціалізований відділ економічної безпеки, який би виконував такі функції:

- Управління ризиками фінансово-економічної безпеки.
- Захист комерційної інформації та моніторинг її використання.
- Розробка антикризових заходів і політик реагування на інциденти.
- Навчання персоналу основам інформаційної безпеки.
- Контроль відповідності внутрішніх політик підприємства законодавчим вимогам.

7. Рекомендовано впровадити гібридні системи шифрування даних із використанням асиметричних (RSA, ECC) і симетричних алгоритмів (AES) для посилення захисту конфіденційної інформації. Особливу увагу слід приділити впровадженню систем моніторингу фішингових атак та корпоративних даних.

8. Запропоновано створити комплексний підхід до оцінки ризиків, що включає ідентифікацію загроз, оцінку їхнього впливу та розробку процедур для їхньої мінімізації. Розробка стратегій повинна враховувати особливості діяльності підприємства та сучасні загрози, такі як кібератаки, витік даних через внутрішні джерела та недоліки в технічному оснащенні.

9. Організація регулярних тренінгів для співробітників з питань кібербезпеки, захисту даних і управління ризиками є обов'язковою складовою підвищення загального рівня безпеки. Особливу увагу слід

приділити роботі з електронною поштою, створенню складних паролів і методам протидії фішинговим атакам.

10. Рекомендовано інтегрувати положення Закону України «Про інформацію» та інших нормативних актів у внутрішні політики підприємства. Зменшить ймовірність порушень і підвищити ефективність управління інформаційними ресурсами.

11. Реалізація запропонованих заходів дозволить суттєво підвищити рівень економічної безпеки підприємства, знизити ризики фінансових втрат та витоку даних, забезпечити відповідність міжнародним стандартам і створити умови для сталого розвитку. Підприємство зможе не лише мінімізувати загрози, а й посилити конкурентні переваги на ринку, забезпечивши стабільність фінансових показників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрощук, Г. О. "Захист комерційної таємниці в США: протидія економічному шпигунству." Наука та інновації 9.2013 (2024): 80-95.

2. Бехтер, Л. А. "Загрози інформаційної безпеки та захист інформації як складова економічної безпеки сільськогосподарських підприємств." Агросвіт 12 (2020): 66-70.

3. Биков, В. Ю., et al. "СИСТЕМА АВТОМАТИЗОВАНОЇ ПЕРЕВІРКИ ПРАВИЛЬНОСТІ РОЗВ'ЯЗАННЯ ЗАДАЧ З ПРОГРАМУВАННЯ." IV МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ: 556.

4. Бондарчук, Наталія Володимирівна, Леся Миколаївна Васільєва, and Альона Вікторівна Міньковська. "Стратегічне управління інноваційним розвитком аграрного підприємства для забезпечення його фінансово-економічної безпеки." Підприємництво та інновації 23 (2022): 37-41.

5. Борисенко, О. С., and А. Г. Тимошенко. "ОГЛЯД МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ХМАРНОМУ СЕРЕДОВИЩІ." Інфокомунікаційні та комп’ютерні технології 1.07 (2024): 31-34.

6. Василина, А. В. Аналіз сучасних мов програмування для захисту програмного забеспечення. Diss. ВНТУ, 2023.

7. Васільєва Л.М., Вітер В.А. «ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ ЯК СКЛАДОВОЇ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ СУБ’ЄКТІВ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ» Збірник тез 2024

8. Вітер В.А., Васільєва Л.М. «ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ, ЯК СКЛАДОВОЇ КОМЕРЦІЙНОЇ ТАЄМНИЦІ ПІДПРИЄМСТВ» Збірник тез 2024

9. Волошко, Максим Миколайович. "Розробка веб-додатка взаємодії з базою даних MySQL за допомогою мови програмування Python та фреймворку fastAPI." (2023).

10. Ворохоб, Максим, et al. "Сучасні перспективи застосування концепції zero trust при побудові політики інформаційної безпеки підприємства." Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка» 1.21 (2023): 223-233.

11. Горбаченко, Станіслав. "Кібербезпека як складова економічної безпеки України." Галицький економічний вісник Тернопільського національного технічного університету 66.5 (2020): 180-186.

12. Дубинська, О. С. "Визначення рівня фінансово-економічної безпеки на підставі аналізу фінансової звітності підприємства." Таврійський науковий вісник. Серія: Економіка 5 (2021): 112-122.

13. Євгеньєв, А. М., А. І. Гальченко, and Д. М. Риков. Фішингові атаки і методи захисту від них. Diss. 2023.

14. Іжболдін, М. М., Васільєва ЛМ. «МЕХАНІЗМИ ТА ПІДХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ ЯК ЕЛЕМЕНТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ» (36) (2023)

15. Касьянова, Н. В., and Н. М. Кравчук. "Управління економічною безпекою підприємства за допомогою цифрових технологій." (2020).

16. Кирилюк, Артем, and Олексій Онацький. "ФІШИНГ ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ АТАК В КІБЕРПРОСТОРІ." РЕДКОЛЕГІЯ (2023).

17. Коваль, П. О. "Кібербезпека–засіб захисту інформації." (2020).

18. Ковальчук, А. М. "Фінансово-економічна безпека підприємства в контексті адаптації до викликів цифрового середовища; Financial and economic security of enterprises in the context of adaptation to the challenges of the digital environment." Економічний вісник Дніпровської політехніки;

Экономический вестник Днепровской политехники; Economic Bulletin of Dnipro University of Technology (2020).

19. Ковальчук, А. М. "Чинники стратегічного управління економічною безпекою підприємства в умовах змін." Економічний вісник Національного технічного університету України «Київський політехнічний інститут» 18 (2021).

20. Комова, С. С., and Т. А. Пушкар. "Кібербезпека в цифровій економіці." Сталий розвиток міст (2023): 66-68.

21. Копилюк, О. І., Ю. В. Тимчишин, and О. М. Музичка. "Фінансова стійкість у системі забезпечення економічної безпеки підприємства." Бізнес Інформ 3 (2021): 81-87.

22. Кравченко, Микола Володимирович, and Николай Владимирович Кравченко. "Шляхи удосконалення управління фінансово-економічною безпекою підприємств аграрного сектору." (2020).

23. Кравченко, О. М. "Організаційно-правові заходи забезпечення охорони конфіденційної інформації та комерційної таємниці бізнесу в Україні." Вчені записки ТНУ імені ВІ Вернадського. Серія: Юридичні науки 3 (2023): 48-53.

24. Кравченко, Олександр Миколайович. "Удосконалення охорони комерційної таємниці та конфіденційної інформації в Україні для інтеграції в Європейське бізнес-середовище." Нове українське право 1 (2022): 211-220.

25. Крамаренко, Катерина, and Олена Вінниченко. "ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ." Сталий розвиток економіки 3 (50) (2024): 344-349.

26. Крихівський, М. В., Т. О. Ваврик, and Л. М. Гобир. "Огляд мов програмування у ракурсі кібербезпеки." Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas 2 (55) (2023): 61-69.

27. Куліков, Василь Михайлович, Вячеслав Віталійович Рябцев, and Святослав Станіславович Паршуков. "Об’єктно-орієнтоване програмування для фахівців з кібербезпеки." (2023).

28. Левченко, О. М., А. О. Левченко, and Т. А. Немченко. "Захист комерційної таємниці в контексті стратегічного управління економічною безпекою організації в умовах цифровізації економіки." Центральноукраїнський науковий вісник. Економічні науки: зб. наук. пр (2021): 20-30.

29. Маслак, Ольга, Ярослава Яковенко. "Забезпечення фінансово-економічної безпеки в умовах цифрової економіки." Вісник Національного технічного університету" Харківський політехнічний інститут"(економічні науки) 3 (2023): 64-67.

30. Маслій, Наталя Дмитрівна, et al. "Модель процесу захисту інформаційних ресурсів та нематеріальних активів підприємств в умовах цифрових трансформацій." (2020).

31. Морозова, А. О. "ОГЛЯД МЕТОДІВ ВИРІШЕННЯ ЗАДАЧІ ШИФРУВАННЯ/ДЕШИФРУВАННЯ ДАНИХ." Редакційна колегія: 50.

32. Нагорна, І. В., and О. О. Степанчук. "Стратегічний аналіз фінансової стійкості підприємства." Ефективна економіка 11 (2020).

33. НІКОЛЬЧУК, Юлія, Богдан НЕБЖИЦЬКИЙ, and Олександр САВЧУК. "Фінансова стійкість як індикатор ефективності використання фінансових ресурсів підприємства." Herald of Khmelnytskyi National University. Economic sciences 314.1 (2023): 220-225.

34. Одношевна О.О., Вітер В.А., Калмиков С.О. «УДОСКОНАЛЕННЯ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ВІД РИЗИКІВ ШАХРАЙСТВА» БІЗНЕСІНФОРМ № 9_2024

35. Одношевна, Ольга Олександрівна, and Ростислав Віталійович Рудой. "Удосконалення обліку витрат на виробництво продукції

рослинництва." Дніпровський державний аграрно-економічний університет, 2022.

36. Одношевна, Ольга Олександрівна. "Підвищення ефективності економічної безпеки сільськогосподарського підприємства за рахунок якісного антикризового управління." (2023).

37. Одношевна, Ольга, Альона Міньковська, and Тетяна Саванчук. "Антикризове управління як елемент удосконалення системи економічної безпеки в сучасних умовах." Економіка та суспільство 49 (2023).

38. Полторак, Анастасія Сергіївна, Анна Леонідівна Сухорукова, and Анна Іванівна Бурковська. "Кібербезпека в системі трансформації управління бізнес-організацією." (2021).

39. Потапюк, І. П., С. С. Мазіленко, and М. О. Прусова. "Фінансово-економічна безпека як основа безпеки підприємства." Цифрова економіка та економічна безпека 2 (02)/ (2022): 156-160.

40. Саванчук, Тетяна Миколаївна, and В. П. Сергієнко. "Ключові напрямки організації системи економічної безпеки аграрного підприємства." Цифрова економіка та економічна безпека 8 (08) (2023): 221-223.

41. Сподіна, Анастасія Олексіївна, and І. О. Тарасенко. "Фінансова стійкість підприємства: сутність та фактори впливу." Міжнародний науковий журнал" Інтернаука" (2022).

42. Стаття 505. Поняття комерційної таємниці Стаття 505. Поняття комерційної таємниці - Цивільний кодекс України Protocol

43. Фізулі-кизи, Саміра Султанова. "ОГЛЯД ТА ПОРІВНЯННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ." Інформаційні моделюючі технології, системи та комплекси (ІМТСК-2023): IV міжнародна науково-практична конференція. 25-26 травня 2023 р., Черкаси, Україна.–Черкаси: Черкаський національний університет

імені Богдана Хмельницького, 2023.–153 с. В матеріалах конференції відображені результати теоретичних та (2023): 76.

44. Хлевицька, Т. Б., and О. Ю. Гусєва. "Управління фінансово-економічною безпекою підприємства засобами реінжинірингу бізнес-процесів." Бізнес інформ 8 (2021): 190-196.

45. Яіцький, Андрій Олександрович, and Марк Геннадійович Сахаров. "ЕФЕКТИВНІ МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ФІШИНГОВИХ АТАК." Problems of science and practice, tasks and ways to solve them 11 (2022): 417.

46. Alam, Mohammad Nazmul, et al. "Phishing attacks detection using machine learning approach." 2020 third international conference on smart systems and inventive technology (ICSSIT). IEEE, 2020.

47. Alkhalil, Zainab, et al. "Phishing attacks: A recent comprehensive study and a new anatomy." Frontiers in Computer Science 3 (2021): 563060.

48. Al-Okaily, Manaf, and Aws Al-Okaily. "Financial data modeling: an analysis of factors influencing big data analytics-driven financial decision quality." Journal of Modelling in Management (2024).

49. Ansari, Meraj Farheen, Pawan Kumar Sharma, and Bibhu Dash. "Prevention of phishing attacks using AI-based Cybersecurity Awareness Training." Prevention 3.6 (2022): 61-72.

50. Begun, Svitlana. "Факторний аналіз фінансових результатів діяльності підприємства: статистична оцінка." Economic journal of Lesya Ukrainka Volyn National University 3.23 (2020): 168-176.

51. Christen, Peter, Thilina Ranbaduge, and Rainer Schnell. "Linking sensitive data." Methods and techniques for practical privacy-preserving information sharing. Cham: Springer (2020).

52. Deepa, Natarajan, et al. "A survey on blockchain for big data: Approaches, opportunities, and future directions." Future Generation Computer Systems 131 (2022): 209-226.

53. Demirkan, Sebahattin, Irem Demirkan, and Andrew McKee. "Blockchain technology in the future of business cyber security and accounting." Journal of Management Analytics 7.2 (2020): 189-208.

54. Florackis, Chris, et al. "Cybersecurity risk." The Review of Financial Studies 36.1 (2023): 351-407.

55. Kozubtsova, L., I. Rudomino-Dusyatska, and V. Snovida. "Обчислення показників ефективності функціонування системи захисту інформації і кібербезпеки." COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION 45 (2021): 19-25.

56. Kulustayeva, Alina, et al. "Financial data reporting analysis of the factors influencing on profitability for insurance companies." Entrepreneurship and sustainability issues 7.3 (2020): 2394.

57. Liang, Meiyi. "Optimization of quantitative financial data analysis system based on deep learning." Complexity 2021.1 (2021): 5527615.

58. Sarker, Iqbal H., et al. "Cybersecurity data science: an overview from machine learning perspective." Journal of Big data 7 (2020): 1-29.

ДОДАТКИ

Додаток А

Розроблений механізм нового програмного забезпечення SkamBlock який буде протидіяти фішинговим атакам на підприємстві