Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет ___інформаційно-аналітичних технологій та менеджменту_____
(повна назва)
Кафедра _ _економічної кібернетики та управління економічною безпекою__
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____

_____Організація системи інформаційної безпеки підприємства в умовах гібридних загроз_____
(тема)

Виконав:
студент _2_ курсу, групи __УФЕБм-21-1__
_____Кодрул Р.Е._____
(прізвище, ініціали)

Спеціальність __073 Менеджмент_____
_____
(код і повна назва спеціальності)
Тип програми _ _освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма ___Управління фінансово-економічною безпекою_____
(повна назва освітньої програми)

Керівник _____доц. Гришко С.В._____
(посада, прізвище, ініціали)

Допускається до захисту

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

2022 р.

Харківський національний університет радіоелектроніки

Факультет__інформаційно-аналітичних технологій та менеджменту_____
(повна назва)

Кафедра_економічної кібернетики та управління економічною безпекою___
(повна назва)

Рівень вищої освіти _____другий (магістерський)_____

Спеціальність _____073 Менеджмент_____
(код і повна назва)

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

Освітня програма _____Управління фінансово-економічною безпекою_____
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____»_____ 2022 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові_____Кодрулу Руслану Едуардовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи _Організація системи інформаційної безпеки підприємства в умовах гібридних загроз_____
_____
затверджена наказом університету від 07_ _листопада_2022 р. № _1452 Ст_____
2. Термін подання студентом роботи до екзаменаційної комісії _19_ __грудня____ 2022 р.
3. Вихідні дані до роботи _Наукові літературні джерела, періодичні видання, фінансова___звітність підприємства, законодавчо-нормативні акти, електронні джерела__
_____
_____
_____
_____
_____
_____

4. Перелік питань, що потрібно опрацювати в роботі _____
Вступ. 1. Теоретичні основи формування інформаційної безпеки підприємств. 2. Аналіз діяльності та управління інформаційною безпекою підприємства АТ «ХАРТРОН». 3. Удосконалення системи інформаційної безпеки підприємства в умовах гібридних загроз. Висновки. Перелік джерел посилання. Додаток._____
_____
_____
_____
_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій_____
1. Об'єкт, предмет, мета і завдання дослідження. _____
2-3. Теоретичні основи формування інформаційної безпеки. _____
4. Організаційна структура АТ «ХАРТРОН». _____
5-10 Аналіз результатів діяльності АТ «ХАРТРОН». _____
11. Послідовність формування системи управління інформаційною безпекою _____ на підприємстві. _____
12. Організаційні заходи АТ «ХАРТРОН», які створюють захист в _____ сфері інформаційної безпеки. _____
13. Система індикаторів слабких сигналів інформаційної безпеки АТ «ХАРТРОН»___

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

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

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Виконання першого розділу роботи	07.11. 2022-12.11. 2022	виконано
2	Виконання другого розділу роботи	13.11. 2022-19.11. 2022	виконано
3	Виконання третього розділу роботи	20.11. 2022-27.11. 2022	виконано
4	Оформлення роботи	28.11. 2022-03.12. 2022	виконано
5	Перевірка роботи на плагіат	04.12. 2022-09.12. 2022	виконано
6	Підготовка доповіді та ілюстративного матеріалу	10.12. 2022-15.12. 2022	виконано
7	Рецензування роботи	16.12.2022-18.12. 2022	виконано
8	Подання роботи до екзаменаційної комісії	19.12.2022	виконано

Дата видачі завдання _07 листопада 2022 р.

Студент _____
(підпис)

Керівник роботи _____ _____доц. Гришко С.В._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна робота: 62 с., 11 табл., 10 рис., 50 джерела, 1 додаток.

ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, БЕЗПЕКА ПІДПРИЄМСТВА, ВРАЗЛИВІСТЬ ПІДПРИЄМСТВА, УПРАВЛІННЯ БЕЗПЕКОЮ, ГІБРИДНІ ЗАГРОЗИ, МОНІТОРИНГ ЗАГРОЗ.

Об’єктом дослідження є система інформаційної безпеки підприємства в умовах гібридних загроз. Предметом дослідження є методи забезпечення інформаційної безпеки.

Метою є теоретичне обґрунтування та розробка практичних рекомендацій з побудови системи інформаційної безпеки підприємства в умовах гібридних загроз.

Розглянуто теоретичні основи формування інформаційної безпеки підприємств, розкрита сутність системного підходу до захисту інформаційної безпеки підприємства, розібрано тему гібридних загроз та їх вплив на інформаційну складову безпеки. Проведено аналіз існуючих підходів та проблем забезпечення інформаційної безпеки в сучасному безпековому ландшафті. Проведено аналіз діяльності та управління інформаційною безпекою підприємства АТ «ХАРТРОН», досліджено існуючі на підприємстві напрями організації інформаційної безпеки. Визначені шляхи удосконалення системи інформаційної безпеки підприємства в умовах гібридних загроз.

ABSTRACT

Master thesis: 62 p., 11 tables, 10 fig., 50 sources, 1 exhibit.

INFORMATION SECURITY, INFORMATION SECURITY SYSTEM, ENTERPRISE SECURITY, ENTERPRISE VULNERABILITY, SECURITY MANAGEMENT, HYBRID THREATS, THREATS MONITORING.

The object of the research is the information security system of the enterprise in conditions of hybrid threats. The subject of research is the methods of ensuring information security.

The goal is theoretical substantiation and development of practical recommendations for building an enterprise information security system in conditions of hybrid threats.

The theoretical foundations of the formation of information security of enterprises are considered, the essence of the systemic approach to the protection of information security of the enterprise is revealed, the topic of hybrid threats and their impact on the information component of security is analyzed. An analysis of existing approaches and problems of ensuring information security in the modern security landscape has been carried out. An analysis of the activity and information security management of "HARTRON" enterprise was carried out, the directions of information security organization existing at the enterprise were investigated. Ways to improve the company's information security system in conditions of hybrid threats are identified.

ЗМІСТ

ВСТУП

В сучасному світі інформаційні технології та засоби використання інформації є важливою частиною існування суспільства. Використання інформаційних систем та засобів складає основу працездатності фінансових, торгових, освітніх та інших структур. Зберігання, обробка, накопичення та обмін інформацією це складний процес, в якому важливо не допустити злочинного використання приватних або секретних даних, яке може привести до тяжких наслідків. Таким чином актуальність безпекових заходів та інформаційної безпеки в цілому набуває все більшого значення, зважаючи на неперервний розвиток технологій роботи з інформацією. Постійне зростання об'ємів інформації, розвиток та вдосконалення засобів зберігання та обробки, активне переведення великих обсягів даних в електронну форму, використання мереж різних типів і масштабів зумовлюють зміну, розвиток та появу нових засобів загрози конфіденційної інформації та спонукають розвиток способів забезпечення інформаційної безпеки на підприємствах.

Інформаційна безпека підприємства здебільшого складається з формування певних принципів, методів та заходів, спрямованих на виявлення, аналіз, запобігання та усунення причин та умов небезпечного впливу на важливу інформацію. Також інформаційна безпека забезпечує питання захисту інформаційного середовища підприємства в умовах імовірності загроз, така можливість досягається за допомогою застосування певних інструментів, які втілюють вчасне попередження про можливі загрози, забезпечують якісну підготовку до протидії, а також реалізують виявлення та ліквідацію інформаційних загроз.

Інформаційна безпека на підприємстві забезпечує застосування комплексних систем заходів, які реалізують протидію зовнішнім та внутрішнім втручанням в інформаційну систему. Такі втручання можуть

привести до збоїв роботи системи управління, незаконного доступу до конфіденційної інформації, її розголошення, та навіть повної втрати працездатності підприємства.

Об’єктом дослідження є система інформаційної безпеки підприємства в умовах гібридних загроз. Предметом дослідження є методи забезпечення інформаційної безпеки.

Метою є теоретичне обґрунтування та розробка практичних рекомендацій з побудови системи інформаційної безпеки підприємства в умовах гібридних загроз.

Основними завданнями дослідження є:

– розглянути теоретичні основи формування інформаційної безпеки підприємств;

– розкрити сучасний стан гібридних загроз та їх впливу на інформаційну складову безпеки;

– провести аналіз існуючих підходів та проблем забезпечення інформаційної безпеки в сучасному безпековому ландшафті;

– проаналізувати діяльність та управління інформаційною безпекою підприємства АТ «ХАРТРОН»;

– описати характеристику діяльності та контуру управління підприємства АТ «ХАРТРОН»;

– провести аналіз існуючих підходів до організації системи інформаційної безпеки підприємства АТ «ХАРТРОН»

– визначити напрямки удосконалення системи інформаційної безпеки в умовах гібридних загроз;

– запропонувати удосконалення системи інформаційної безпеки підприємства АТ «ХАРТРОН» в умовах гібридних загроз.

Методичною основою для проведення дослідження були наукові літературні джерела, періодичні видання, фінансова звітність підприємства, законодавчо-нормативні акти, електронні джерела.

Під час дослідження були використані методи аналізу та створення інформації, що описує діяльність підприємства з забезпечення безпеки його інформаційного середовища, порівняння та узагальнення показників безпеки інформаційної діяльності підприємства, створення висновків, що випливають з результатів аналізу на базі становища під час забезпечення інформаційної безпеки підприємств.

Значення практичного характеру отриманих результатів полягає у використані запропонованих практичних рекомендацій підприємствами різних галузей та типів для забезпечення захисту інформаційних систем в умовах гібридних загроз.

Апробація результатів дослідження. Основні теоретичні положення і практичні результати проведених досліджень, висновки і рекомендації, які викладені в роботі, доповідались на ІІІ Міжнародній науково-практичній конференції «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта» (Харків. 1 листоп. 2022) та ІІІ Міжнародній науково практичній конференції «Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці» (Київ, 22 листоп. 2022 р.).

Acknowledgment. Під час дослідження були використані матеріали Еразмус+ проєкту WARN «Academic Response to Hybrid Threats» (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP), який фінансується програмою Європейського Союзу Erasmus+.

Disclaimer: «The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein».

Публікації. Результати досліджень опубліковано у 2 наукових працях в якості 2 матеріалів конференцій (тези доповідей).

1 ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1 Системний підхід до захисту інформаційної безпеки бізнесу

Інформаційна безпека підприємства - це певний стан захищеності усіх інформаційних систем підприємства, при якому забезпечується конфіденційність, доступність та цілісність зберігаємої інформації, а також її використання в інтересах розвитку підприємства. Також це втілений комплекс заходів, які спрямовані на забезпечення захищеності інформації від несанкціонованого доступу. Інформаційна безпека характеризується ступенем захищеності та стійкістю до небезпечних інформаційних впливів як до впровадження нової, так і до отримання зберігаємої інформації. Інформаційна безпека – це стан захищеності інформаційної середи об’єкта, при якому досягається такий інформаційний розвиток, його технічні, інтелектуальні та соціально-політичні аспекти, за умови якого сторонні інформаційні впливи не спроможні завдати йому суттєвої шкоди [1].

Виступаючи одним з основних напрямків методології спеціального наукового пізнання, системний підхід сприяє формуванню суті досліджуваних процесів, розкладаючи їх на складові. Таким чином можна сформулювати його мету і основне завдання у дослідженнях певних об’єктів як складних систем взаємопов’язаних компонентів. Для виявлення значення системного підходу потрібно детально зрозуміти сутність поняття «система», розділивши її на основні властивості: багатокомпонентність, залежність системи від її окремих елементів, залежність від зовнішнього середовища, ієрархічність системи.

Багатокомпонентність характеризує те, що будь-яка система складається з сукупності взаємопов'язаних елементів. Система є набором складових елементів, які мають певну залежність або зв'язок між сосбою, а

також мають залежність від розташування у системі та можуть створювати підсистеми.

Залежність системи від її окремих елементів, їх властивостей, поведінки та структури. Система є залежною від складових, сутність системи може змінюватись разом із зміною окремих частин системи, складові системи формують її сутність, опис властивостей та характеристик складових допомагає описати загальні риси системи. Треба розуміти, що властивості системи не обов'язково визначаються своїми елементами, таким чином, систему не можна розглядати лише як сукупність елементів, так само, розглядаючи окремо різні частини системи, не можливо описати загальні системні властивості.

Так само, як і залежність системи від внутрішніх особливостей, потрібно зважати на спроможність системи до змін відносно чинників зовнішнього середовища. Таким чином система входить в стан взаємодії, реагуючи на зовнішні впливи в цілому і також всіма складовими елементами.

Ієрархічність системи визначає спроможність системи до набуття такого стану, в якому кожен рівень деталізації представляє собою меньшу за масштабом систему. Таким чином системи інформаційної безпеки, в залежності від масштабу впливу, можуть розглядатись як суперсистеми, великі системи, підсистеми та окремі їх елементи [2-6].

В наш час стрімкого розвитку технологій в інформаційному середовищі, виникає питання актуальності методів системного аналізу, потреба у переосмисленні існуючіх підходів до створення та розвитку інформаційних технологій. Це призводить до того, що проблеми забезпечення інформаційної безпеки повинні розглядатися як складові елементи системи безпеки, під час створення сучасних систем забезпечення інформаційної безпеки як на етапі проектування, так і на всіх наступних стадіях експлуатації і підтримки.

Актуальність системного підходу можна пояснити його метою у контексті застосування для системи інформаційної безпеки підприємства, він має на меті групування та систематизування усіх факторів, які створюють, або можуть створювати сприятливі умови для безпечного функціонування та розвитку інформаційного середовища підприємства. Системний підхід пропонує підходи до вирішення типових проблем та забезпечує механізми реагування на нові проблемі, шляхом аналізу конкретних складових, дій, процесів та їх зав'язків у інформаційний системі, за допомогою комплексного урахування ключових чинників. При вирішенні безпекових проблем під час функціонування підприємства, сутність системного підходу розкривається в аспектах діяльності колективу, деталях роботи підприємства, впливі внутрішніх та зовнішніх факторів, які мають розглядатись в якості динамічної системи, а сукупність залежностей та зв'язків сприяє виявленню оптимальних шляхів оптимізації та розвитку цієї системи. Також можна розглядати системний підхід як напрям методології наукового пізнання, в такому випадку він базується на розгляд об'єктів як систем, таким чином він орієнтує на розкриття цілісності об'єкта, виявлення різноманітних зв'язків у ньому, а також зведення їх в цілісну теоретичну картину [7].

Системний підхід в організації системи захисту інформації базується на використанні та поєднанні взаємопов'язаних організаційних, адміністративних, апаратних, програмних, матеріальних та інших властивостей системи, оптимально впроваджених та підтверджених на практиці використання систем захисту на всіх етапах технологічного шляху зберігання, обробки та використання інформації.

Сутність підходу полягає у створенні комплекса методів, які дозволяють описувати об'єкт як систему сукупності взаємопов'язаних чи взаємодіючих компонентів. Таким чином, системний підхід створює умови для забезпечення інформаційної безпеки шляхом комплексної реалізації

роботи окремих компонентів та поєднання їх, з урахуванням вимог до структурних характеристик. Системний підхід потребує наявності кваліфікованих співробітників, які виконують фактичну реалізацію методів системного підходу. Системні аналітики реалізують засоби забезпечення інформаційної безпеки та контролюють їх роботу, вони проектують, створюють та використовують комп'ютерні системи управління, проводять детальний аналіз бізнес-процесів та проектують шляхи їх автоматизації, розробляють технічні завдання та формують специфікації, формують аналітичні звіти [8].

В контексті сучасних питань інформаційного середовища концепція безпеки полягає в тому, що пошук єдиного універсального засобу захисту заміняється створенням комплексних підходів поєднання різних засобів захисту інформації, які зазвичай покривають проблеми:

- - нормативно-правового аспекту захисту інформації;
- застосування різноманітних засобів, способів та методів захисту;
- організацію органів та виконавців.

Формування захисту інформації на підприємстві виступає системою засобів, методів та відповідних заходів, що виконуються з метою регулярного забезпечення достатнього рівня надійності інформаційного середовища підприємства. Системний характер захисту сприяє отримання комплексних рішень протидії інформаційним загрозам, різноманітні види захисту інформації мають працювати посилюючи один одного в складі цілісної загальної системи безпеки підприємства, виконуючи задачі з забезпечення усіх аспектів безпеки інформаційної системи. Системність безпеки забезпечує одночасно і функціонування фактичних механізмів захисту, і управління механізмами захисту інформації також, виходячи з цього, є велика потреба у організації якісної системи управління захистом інформації та підготовка кваліфікованого персоналу [9-10].

З питання доступу до інформації та обмежень в використанні систем безпеки, важливим є визначення кордонів і делегування повноважень в сумісному доступі і виконанні інформаційних задач, виявлення неочікуваних використань, прогнозування загроз та усування їх наслідків, з можливістю гнучких змін частин системи при умовах проблем з несанкціонованим доступом до інформації.

Загальні риси системи інформаційної безпеки визначаються об’єктом захисту, функціональними завданнями та фактичними елементами організаційної структури, також нормативною базою, яка необхідна для її формування та здійснення захисту. Виходячи з цього, система економічної безпеки підприємства виражається в сукупності об’єкта, засобів захисту, нормативної бази та організаційної структури її забезпечення. Втілюється вона в комплексі пов’язаних заходів, органів та підрозділів, які забезпечують захист всіх функціональних складових підприємства від можливих зовнішніх та внутрішніх загроз.

Системний підхід до управлінського процесу будь-якого підприємства базується на чітких принципах, які забезпечують реалізацію сутності системного підходу. Такі принципи наведені на рисунку 1.1.

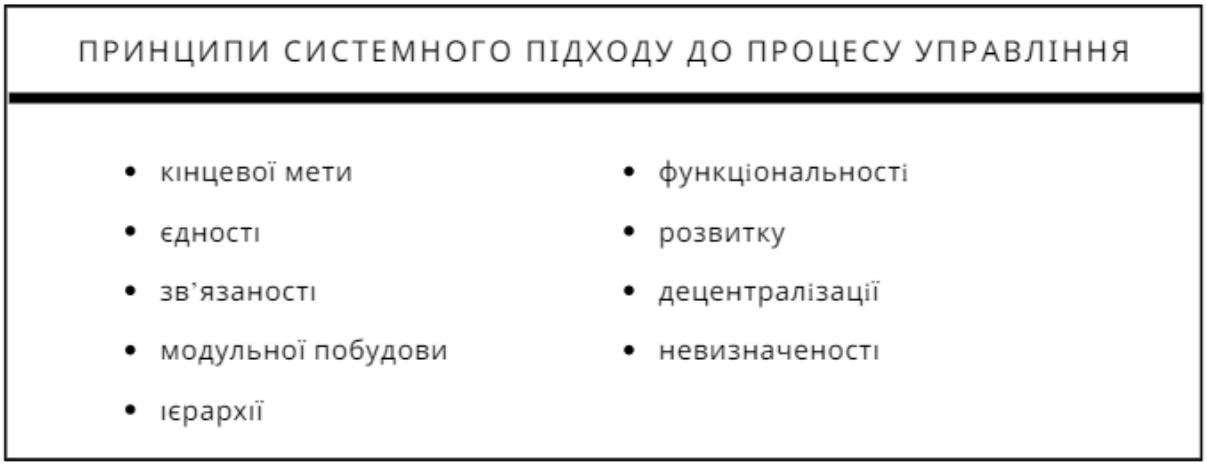

Рисунок 1.1 – Принципи системного підходу до процесу управління

Принцип кінцевої мети – це принцип, який визначає абсолютним пріоритетом досягнення кінцевої мети. Принцип єдності визначається тим, що система розглядається і як єдине ціле і за сукупністю своїх елементів. Принцип зв'язаності визначається у вивчанні кожного окремого елементу системи за зв'язками між собою та з навколишнім середовищем. Модульної побудови – це принцип у якому в системі виділяють окремі модулі та розглядають їх у сукупності та взаємодії. Принцип ієрархії пропонує втілити ієрархію елементів та здійснити їх ранжування. Принцип функціональності – розглядає структури і функції, визначаючи пріоритетність функцій над структурою. Принцип розвитку враховує зміни системи, її здатність до розвитку та розширення, заміни окремих частин. Принцип децентралізації – поєднання рішень, які приймаються, та виконують керування централізацією і децентралізацією. Принцип невизначеності – це врахування невизначеності та випадковості в системі для подальшого прийняття управлінських рішень.

Для ефективного управління інформаційною безпекою підприємства потрібно враховувати загальні принципи управління інформаційного середовища та розробляти ефективні стратегії розвитку. В залежності від повноти наявної інформації, формуються стратегії, і від деталей та умов реалізації стратегії можуть суттєво відрізнятись на перших етапах планування та у кінцевому варіанті реалізації. Тому якість безпекового менеджменту, процесу реалізації стратегії, отримання інформації та її аналізу, так само, своєчасності і обґрунтованих управлінських рішень, створення спроможної до фактичних дій інформаційної системи з аналітичними можливостями буде впливати на забезпечення безпеки підприємства [11-14].

В контексті безпеки підприємства та інформації, яка використовується в його діяльності, ознаки системного підходу описують характер взаємодії з інформацією та частинами інформаційної системи. Одна з характерних ознак системного підходу - це одночасне охоплення великої кількості завдань під

час проектування та виконання потокової діяльності. Також системному підходу притаманний високий рівень типізації та стандартизації розроблених рішень. Уявлення про структуру інформаційної системи відбувається за комплексним розкриттям аспектів системи, яка зазвичай формується з декількох видів компонентів, та, за можливості, реалізує їх автономну працездатність. Ключову роль в системному підході відіграє реалізація безпечних та зручних у використанні баз даних та систем доступу до даних.

В загальному висновку, системний підхід дозволяє реалізувати комплексну та захищену систему безпеки інформації. Він допомагає знаходити нові та нестандартні вирішення як звичних проблем так і новітніх форм загрози інформації, аналізувати конкретні спроможності системи, дії в внутрішньому та навколишньому середовищі, визначати задачі та цілі, на базі комплексного вивчення чинників інформаційного середовища. Інформаційна безпека підприємства реалізує комплексний стан захищеності інформаційних систем підприємства, який забезпечує конфіденційність, доступність та цілісність зберігаємої інформації та використання її в інтересах розвитку підприємства, вона втілює комплекс заходів, які спрямовані на забезпечення захищеності інформації від злочинного впливу. Потреба використання системного підходу закладається у тому, що своєю метою він ставить угрупування всіх суттєво важливих факторів безпекового становища, для створення позитивних умов безпечного функціонування та розвитку діяльності підприємства. Таким чином, без відповідного захисту інформації, за сучасних умов конкуренції, неможлива ефективна економічна діяльність.

1.2 Гібридні загрози та їх вплив на інформаційну складову безпеки

Гібридні загрози за своєю сутністю стосуються дій, метою яких заподіяння шкоди або підрив діяльності цілі, на яку вони впливають. Гібридна війна — це процес спрямований на встановлення зовнішнього контролю над об'єктом управління за допомогою встановлення тотальної залежності об’єкта в питаннях управління з використанням інформаційних засобів в якості одного з головних інструмента. В міжнародному контексті гібридну війну можна розглядати як прагнення однієї держави впливати на іншу задля повного підкорення, використовуючи для цього політичні, економічні та інформаційні інструменти. Гібридні загрози можна відноситися до методів, які використовують окремі державні або недержавні суб'єкти з метою покращення власних геополітичних та інших інтересів, втілення стратегій та досягнення цілей. В контексті війни, гібридні загрози виступають противником, який використовує як звичайне озброєння, так і, одночасно, адаптуючи спільне використання, застосовує терористичні засоби, злочинну поведінку в зоні бойових дій та інформаційному просторі для досягнення своїх політичних цілей. Таким чином гібридність загроз може відноситися до воєнної ситуації, до стратегії та тактики противника, а також до типу сил і засобів, створених та розвинутих державою [15-17].

В сучасній війні гібридні дії противника характеризуються по-перше неоднозначністю типів та засобів застосування, а також контекстів. Суб’єкти гібридних загроз не чітко підпорядковуються звичним форматам міжнародної політики, вони розмиваються у інформаційному просторі та виконують дії як з зовнішніми так і з внутрішніми державними і недержавними структурами, використовують законні і злочинні засоби досягнення результатів.

Сучасний стан безпеки підприємницької діяльності в Україні знаходиться у постійному контексті існування різнопланових форм гібридних загроз. Під час активної фази гібридної війни противник

використовує економічні, соціально-психологічні та диверсійні форми злочинної діяльності в середині країни, це не може не впливати на безпековий стан підприємств та регулярну появу нових загроз. Характеристики впливу цих компонентів та міра їх використання у протистоянні залежать від фактичного рівня розвитку економіки та технологій сторін конфлікту. Гібридні впливи реалізуються завдяки активному використанню технологічно передових систем та тактиці їх застосування, яка характеризується активною роботою на межі можливостей. Таким чином, гібридні сили мають перевагу над класичними загрозами, вони мають перевагу у тому, що стирають традиційні уявлення та практики війни, виграючи у комплексності та прихованості нанесеної шкоди.

В Україні під загрозою гібридної війни опинились фактично усі сфери життєдіяльності, такі як, економіка, політика, культура, інформаційне споживання, навіть ідентичність. Сильна прив'язаність до російського ринку деяких секторів вітчизняного господарства, проблемно розвинуті альтернативні джерела постачання ресурсів покладають питання національної безпеки [18-21].

Очевидно, що в таких умовах необхідно переосмислення підходів до створення та розвитку інформаційних систем та технологій і питання інформаційної безпеки повинні розглядатися як складові елементи при створенні інформаційних систем, починаючи з моменту їх проектування та на всіх наступних стадіях виробництва і підтримки. Для досягнення такого рівня реалізації дуже важливим є вирішення фундаментальних завдань: забезпечити обмін інформацією в режимі реального часу, забезпечити широке співробітництво в області кібербезпеки, забезпечити використання інтегрованих технологічних платформ.

Темпи розвитку цифрового світу продовжують зростати, потрібно швидко реагувати на нові загрози і виявляти слабкі місця в системі інформаційної безпеки. Ефективна кібербезпека повинна ґрунтуватися на принципах якісної співпраці організації або держави, щоби вчитися один у одного. Розробники інформаційних систем мають орієнтуватись на створення

інтегрованих технологічних платформ та впровадження нових підходів до їх розроблення, що зможе забезпечити безпечне функціювання інформаційних систем [22-23].

Змістовне розкриття процесів забезпечення інформаційної безпеки підприємства в умовах гібридних загроз передбачає комплексне дослідження поняття потенціалу інформаційної безпеки, за виконання якого потрібна масштабована вказівка рівня держави, регіону або підприємство, на якому вони розглядається. Необхідно зазначити, що контекст рівнів може впливати на темпи розвитку та росту. Важливим є визначення факторів, які мають вплив на розвиток потенціалу інформаційної безпеки підприємства, зазвичай, вони не обмежуються рівнем підприємства, за умови впливу гібридних загроз. Система забезпечення інформаційної безпеки підприємства повинна являти собою гнучку систему з чітко визначеними елементами, така система обов’язково має змінюватися і адаптуватися до зовнішніх та внутрішніх умов та загроз ефективному функціонуванню підприємства [24-28].

Виходячи з цього, ми бачимо, що в умовах гібридної війни першочергової актуальності набувають проблеми насильницького розв'язання конфліктів. Вони характеризується інтенсивністю і широким застосуванням різноманітних методів прямої та непрямої агресії, а також здатністю залучати велику кількість людей, негативно впливаючи на систему державної стабільності та інформаційну безпеку країни в цілому та підприємств.

1.3 Аналіз існуючих підходів та проблем забезпечення інформаційної безпеки в сучасному безпековому ландшафті

Поняття інформаційної безпеки не може обмежуватись лише технічною безпекою електронних інформаційних систем та інформації у електронному вигляді. Якісна безпека досягається при забезпеченні захищеного зберігання та використання даних незалежно від виду носія та форми, у якій вони перебувають, від електронних баз даних до папірця з паролем та знань співробітників, які мають доступ до конфіденційної інформації. Важливість реалізації якісної системи забезпечення інформаційної безпеки мотивується необхідністю створення умов ефективного функціонування підприємства, запобігання можливим загрозам безпеки, захист інтересів підприємства, недопущення розголошення, втрати, витоку, та знищення конфіденційної інформації.

Потенційні загрози, які постають перед системою інформаційної безпеки зазвичай розділяють на внутрішні та зовнішні. Внутрішньою загрозою може бути, наприклад, крадіжка або знищення інформації співробітником компанії, зараження комп’ютерної системи шкідливим програмним забезпеченням, завдання фізичного пошкодження комп’ютерам або серверам. Причинами таких дій можуть виступати як проблеми персональних відносин між співробітниками так і незадоволення співробітниками заробітною платою та умовами праці, або навіть шпигунська діяльність співробітників на користь інших компаній. Зовнішніми загрозами можуть бути копіювання цінних документів, викрадення або пошкодження носіїв даних, викрадення інформації яка передається через Інтернет, передача інформації до конкурентних компаній або переманювання співробітників до конкурентів [29-30].

Таким чином, в залежності від специфіки носіїв інформації та способів її використання, існує потреба в реалізації фізичних засобів захисту інформації. Фізичні засоби захисту інформації як втілюються для забезпечення протипожежної безпеки приміщень, захисту від проникнення правопорушників приміщення, контролю за доступом співробітників до інформації у приміщенні зберігання [31].

В наш час, коли аналогові носії даних все ще використовуються, але цифрові технології розвиваються дуже активно, великої актуальності і ваги набувають саме програмні засоби забезпечення безпеки інформації. Таким чином, спеціальні програми, що часто являються частиною програмного забезпечення системи зберігання та обробки інформації, пропонують можливості захисту від несанкціонованого передавання даних через Інтернет, а також протидії перехопленню інформації.

Доволі часто причиною небезпеки зберіганню інформації є шкідливе програмне забезпечення чи віруси. Вони можуть перехоплювати приватні дані, паролі, секретну інформацію, шукати дані в системі або на комп’ютері, змінювати або знищувати дані та програми в комп’ютерних системах підприємства. Боротьба з вірусними програмами залежить від типу носія та способу передачі віруса на комп’ютер, це може бути як флешка з шкідливою програмою так і фальшивий сайт, який може перехопити важливу інформацію.

Зважаючи на різноманіття способів застосування та видів шкідливого програмного забезпечення, серед програмних засобів захисту інформації широкого застосування набувають антивірусні програми, які забезпечують комп’ютерні системи підприємств, а також персональні комп’ютери співробітників, можливістю виявлення та знищення вірусів. Також важливою складовою захисту від шкідливих програм є навчання співробітників безпечним методам користування програмами, це можуть бути як прості правила, наприклад не переходити по невідомим посиланням

або робити складний пароль, так і доволі якісні навички користування специфічними програмами, використання двофакторної автентифікації та вміння за зовнішніми ознаками визначати шахрайські підробні сайти.

Але на практиці одне лиш використання антивірусної програми або наявність вогнегасника у приміщенні архіву не побудують систему інформаційної безпеки підприємства, задля її реалізації потрібен комплексний підхід до захисту інформації підприємства. Використання декількох методів на практиці не забезпечить підприємство задовільним рівнем захисту. Інформаційний захист фактично здійснюється шляхами адміністративної організації та шляхом впровадження програмного забезпечення. Опис адміністративного та програмного шляхів наведено на рисунку 1.2.

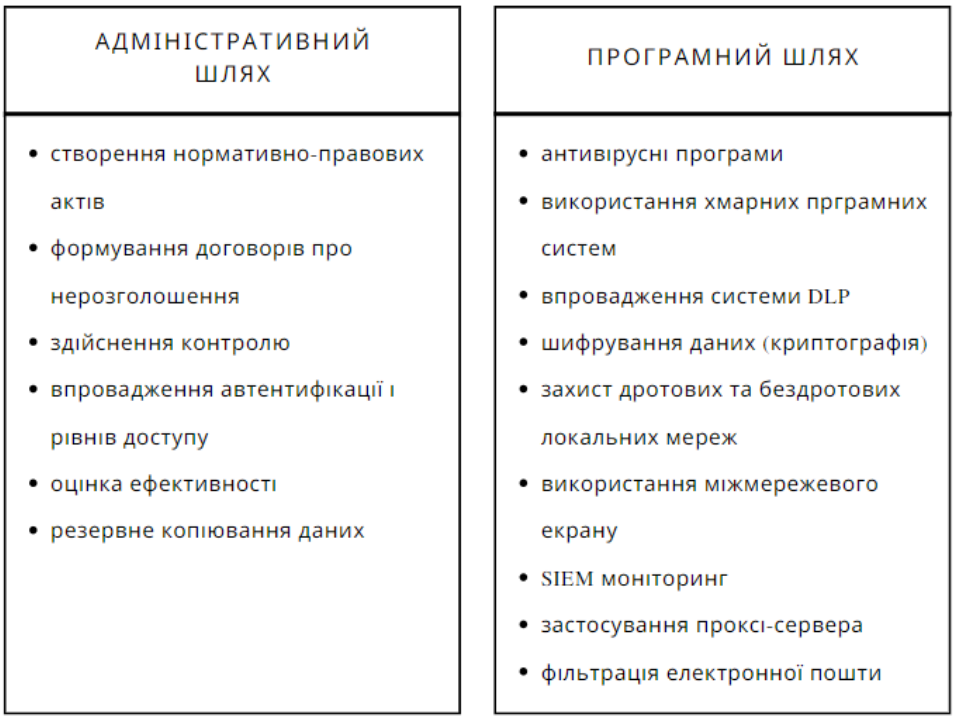

Рисунок 1.2 – Адміністративний та програмний шляхи інформаційного захисту

Адміністративний шлях включає формується за допомогою створення в рамках підприємства нормативно-правових актів та підписання договорів

про нерозголошення, правила користування та передачі отриманої інформації з співробітниками. Важливим є і впровадження відповідного контролю за виконанням усіх внутрішніх нормативних документів та впровадження системи автентифікації та відповідних рівнів доступу до інформації різних ступенів секретності, задля уникнення зайвого витоку конфіденційної інформації Впровадження механізмів оцінки працездатності та ефективності роботи системи управління інформаційною безпекою підприємства та своєчасний розвиток системи за результатами оцінки. Регулярне резервне копіювання даних виконується для відновлення інформаційної системи в випадку збою, атаки або падіння.

Шлях використання програмного забезпечення, в свою чергу, реалізується за допомогою впровадження сучасних програм, яких існує величезна кількість і вони постійно розвиваються та покращують характеристики. Цей шлях реалізується за допомогою, в тому числі, антивірусних програм. Вони регулярно перевіряють комп’ютер на наявність шкідливих програм. У разі виявлення загрози, повідомляють про це користувача або одразу блокують її. Використання хмарних програмних систем може бути ефективним для захисту даних від вірусів та можуть нівелювати нестачу потужності комп’ютерів. На пристрій встановлюється проста програма, яка забезпечує захищений зв’язок з хмарою, де і відбувається зберігання та обробка даних. Впровадження системи DLP (Data Leak Prevention), такі системи аналізують усю вхідну та вихідну інформацію та за допомогою неї виявляють підозрілі операції та ризики, вирішують проблему витоку даних. Реалізація таких системи доволі складна та фінансово витратна задача, проте забезпечує високий рівень ефективності. Існує багато надійних систем шифрування даних, які реалізують безпечну передачу та роблять майже неможливим перехоплення такої інформації. Важливою є і реалізація захисту дротових та бездротових локальних мереж сучасними методами, також захист доступу до глобальних мереж.

Використання міжмережевого екрану для блокування та фільтрації трафіку забезпечує відокремлення корпоративної мережі від глобальної та встановлює певні обмеження з можливістю виходу в інтернет. SIEM моніторинг фіксує та зберігає всі, отримані від мережевих пристроїв та частин системи, логи для їх аналізу та виявлення шкідливих дій. Застосування проксі-сервера прискорює відгук на запити до затребуваних ресурсів а також дозволяє захищати клієнтський комп'ютер від деяких можливих мережевих атак і допомагає зберігати анонімність клієнта. Існують програмні засоби, які фільтрують та переглядають вміст листів електронної пошти, відсікають СПАМ, виявляють заражені вірусами листи, також блокують відсилання файлів з конфіденційною інформацією.

Концептуально безпека підприємства безперервно розвивається реагуючи на внутрішні та зовнішні фактори наявних інформаційних загроз. Сучасний безпековий ландшафт також регулярно змінюється, це залежить від великої кількості факторів, серед яких виділяються фактори появи гібридних впливів та сприяння розвитку гібридних загроз, вони втілюються, по-перше, посиленні такого поняття як "влада слабких" та, по-друге, у зміні самої природи протистояння між державами. Приклади таких змін наведено на рисунку 1.3.

Перша тенденція пов'язана із переходом від рівного протистояння, яке визначається владою, яка базується на ресурсах до асиметричного протистояння. Такий тип влади дозволяє досягати цілей протистояння, не маючи достатніх економічних переваг. Таким чином, «влада слабких», дозволяє гравцям отримувати певні переваги.

Рисунок 1.3 – Зміни безпекового ландшафту

Слабший учасник протистояння зможе кинути виклик сильнішому, за рахунок вмілого поєднання та синхронізації різних інструментів впливу. Комбінуючи інструменти та змінюючи рівень впливу кожного з них, слабший може залишатися малопомітним у своїй діяльності, але при цьому досягати більшого результату, в порівнянні з використанням одного інструмента з максимальною потужністю застосування.

Сучасне протистояння між державами витікає з довготривалого суперництва між комунізмом і капіталізмом, яке базувалося на конкуренції економічних систем, з нього з’явився новий формат протистояння між державами. Цей формат створює бажання з боку авторитарних держав отримати, відновити або переглянути свій статус та посилити свій вплив на інші країни, зробивши виклик нормативному світовому порядку.

Виходячи з цього, актуальна ситуація протистоянь між державами мотивує появу нових видів гібридних загроз, а посилення "влади слабких" – створює можливості для розвитку та вдосконалення засобів гібридних загроз. В умовах такого протистояння ідея гібридності, зазвичай, стає дієвою тактикою для тих, хто не має достатніх економічних спроможностей для досягнення та просування своїх стратегічних інтересів іншим чином [32-34].

Таким чином, можна зазначити, що відношення поняття інформаційної безпеки підприємства щодо внутрішньої інформації, інформаційних систем та засобів як до об’єктів безпеки, буде доречним поділити на такі складові, як доступність, цілісність та конфіденційність. Доступність можна розглядати як можливість за визначений час отримати певну інформаційну послугу. Цілісність визначається захищеністю інформації від руйнування та несанкціонованого змінювання, релевантністю, чіткістю та сумісністю інформації. Конфіденційність - це захищеність від несанкціонованого доступу. З позиції інформаційних технологій захисту інформації можна розглянути інформаційну безпеку як комплексну систему заходів, задача якої є забезпечувати спроможність виявляти вразливі місця інформаційної системи підприємства, визначати небезпеки, які загрожують їй, а також формувати методи нейтралізації виявлених загроз [35-36].

Розглянуто теоретичні основи формування інформаційної безпеки підприємств, розкрита сутність системного підходу до захисту інформаційної безпеки підприємства, розібрано тему гібридних загроз та їх вплив на інформаційну складову безпеки. Проведено аналіз існуючих підходів та проблем забезпечення інформаційної безпеки в сучасному безпековому ландшафті. Підсумовуючи, можна зазначити, що гібридні загрози є одним з найбільших викликів оточуючому середовищу в глобальному масштабі.

2 АНАЛІЗ ДІЯЛЬНОСТІ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА АТ «ХАРТРОН»

2.1 Характеристика діяльності та контуру управління підприємства АТ «ХАРТРОН»

Акціонерного товариства «ХАРТРОН» було створено в 1959 році. Підприємства АТ «ХАРТРОН» працюють в ракетно-космічній галузі, енергетиці, залізничному транспорті. Ракетно-космічний напрямок у діяльності АТ «ХАРТРОН» визначається пріоритетним. На ринку космічних технологій підприємство продовжує займати лідируючу, а в деяких аспектах навіть монопольну позицію.

АТ «ХАРТРОН» представлено у холдинговій структурі, до складу якої входять керуюча компанія, акціонерне товариство, а також 9 інших підприємств, які було створено за участю керуючої компанії. Організаційно підприємство знаходиться у підпорядковані Державному космічному агентству України, якому належить пакет акцій. Керуюча компанія АТ «ХАРТРОН» є науковою організацією, яка має ліцензію ДКАУ на виконання робіт у космічній сфері. Також в інтересах підприємств керуюча компанія здійснює взаємодію з ДКАУ, міністерствами і відомствами України та партнерами в інших країнах, веде діяльність з координації робіт дочірніх підприємств, пошуку нових замовлень. Підприємства, що входять до складу АТ «ХАРТРОН», розташовані в Харкові, Запоріжжі та Бердянську. Кожне підприємство є юридичною особою. За організаційною структурою до складу АТ «ХАРТРОН» входять 9 підприємств, які займаються особистими напрямками діяльності.

НВП ХАРТРОН-АРКОС ЛТД займається розробкою систем управління для ракетних комплексів та космічних апаратів, також автоматизованих систем управління та систем діагностики, які використовуються на атомних електростанціях.

НВП ХАРТРОН-ПЛАНТ ЛТД відповідає за виготовлення апаратури систем управління ракетних комплексів та космічних апаратів, апаратури для атомних електростанцій та товарів народного споживання.

ТОВ НВП ХАРТРОН-ЮКОМ реалізує розробку та виготовлення апаратури для систем управління космічних апаратів, телеметричної апаратури, волоконно-оптичних ліній зв'язку, систем телемеханіки і автоматизованих систем управління технологічними процесами для нафтогазової галузі.

НВП ХАРТОН-ЕНЕРГО ЛТД – це підприємство, яке займається розробкою та виготовленням приладів автоматизації для атомних і теплових електростанцій, також газових аналізаторів.

ТОВ НВП ХАРТРОН-АСКОНД ЛТД реалізує розробку підсистем системи управління і виробництво комп'ютерів і периферійного обладнання.

Підприємство ТОВ ВЕСТРОН створене спільно з американською компанією «Westinghouse», відповідає за проектування, виготовлення та впровадження автоматизованих систем управління технологічними процесами для атомних, теплових електростанцій та інших промислових об'єктів.

ТОВ НВП ХАРТРОН-ІНКОР ЛТД займається розробкою та виготовленням апаратури релейного захисту та автоматики для об'єктів енергетики та вокзальної автоматики.

Підприємство НВП ХАРТРОН-ЕКСПРЕС ЛТД розробляє та виготовляє електрообладнання для рухомого складу залізниць і вокзалів.

До складу входить підприємство ТОВ ХАРТРОН-ВІОЛІС, яке є дитячим оздоровчим комплексом.

Також підприємство АТ «ХАРТРОН» має в своїй структурно-організаційній системі служби:

- головного механіка;
- головного електрика;

- планування організації праці і заробітної платні;
- відділ технічного контролю;
- відділ збуту;
- спец. конструкторське технологічне бюро;
- охорони праці та техніки безпеки;
- економіки і управління;
- маркетингу;
- комерційної діяльності;
- забезпечення якості.

На рис. 2.1 наведена типова структурно-організаційна схема науково-виробничого підприємства в складі АТ «ХАРТРОН» на прикладі НВП ХАРТРОН-АРКОС ЛТД.

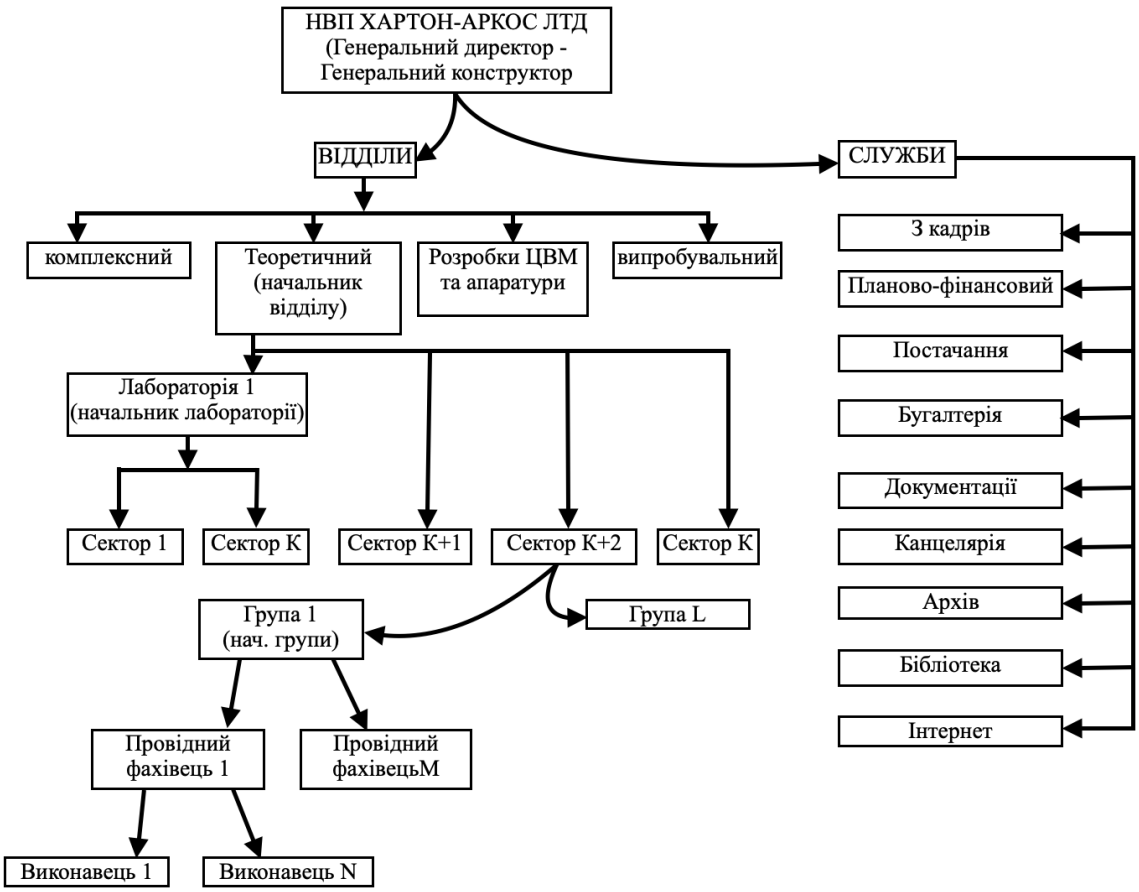

Рисунок 2.1 – Структура НВП ХАРТРОН-АРКОС ЛТД АТ «ХАРТРОН»

АТ «ХАРТРОН» було найбільшим у СРСР розробником і виробником систем керування ракет стратегічного призначення та космічних апаратів, а також ракет-носіїв космічних апаратів. Ракети-носії із системами керування, розробленими підприємством, вивели на орбіту близько 1000 космічних апаратів, у тому числі і перший штучний супутник Землі, виготовлений в Україні. За роки незалежності України була здійснена глибока диверсифікація виробництва по видах діяльності і по переліку основних замовників, також була проведена реструктуризація підприємства.

Згідно зі статутом акціонерне товариство «ХАРТРОН» є юридичною особою з новим найменуванням у результаті прийнятого рішення про зміну типу товариства з публічного акціонерного товариства на приватне акціонерне товариство та про зміну найменування з ПУБЛІЧНОГО АКЦІОНЕРНОГО ТОВАРИСТВА «ХАРТРОН» на АКЦІОНЕРНЕ ТОВАРИСТВО «ХАРТРОН». Засновником Товариства є держава в особі Фонду державного майна України.

Основними предметами діяльності Товариства виступають:

− системний аналіз і визначення найбільш перспективних напрямків і тенденцій розвитку систем і комплексів керування;

− розроблення, випробування, виробництво, експлуатація складових частин ракетоносіїв, космічних апаратів, наземної космічної інфраструктури;

− проектні роботи, розробка, випробування систем автоматичного керування;

− виробництво, монтаж технологічного обладнання, пусконалагоджувальні роботи;

− виробництво медичного обладнання, обладнання для переробки сільськогосподарської продукції, пожежної техніки, складної побутової техніки і товарів народного споживання;

− математичне і фізичне моделювання процесів керування та технологічних процесів, розробка технічної документації на бортову і наземну апаратуру для спецтехніки, а також на медичну і побутову апаратуру;

− впровадження ноу-хау, науково-технічних розробок організацій, установ та відомств у народне господарство України;

− фундаментальні, пошукові і системні дослідження з розвитку систем керування народногосподарського, наукового та оборонного призначення;

− оренда, створення власних та/або спільних каналів зв'язку, їх експлуатація;

− надання в оренду власного нерухомого майна;

− інша діяльність, що сприяє досягненню мети Товариства і не заборонена діючим законодавством України.

Основною метою діяльності є одержання прибутку на основі здійснення виробничої, комерційної та посередницької діяльності. Основними видами діяльності є дослідження й експериментальні розробки у сфері природничих і технічних наук, ІТ-галузі, установленні та монтажі машин і технічного обладнання, управління корпоративними правами [37].

2.2 Аналіз основних показників діяльності підприємства АТ «ХАРТРОН»

Проведення економічного аналізу є важливою складовою системи управління підприємством, втілюється шляхами фінансового менеджменту, а також економічними відносинами із партнерами та конкурентами. За

результатами економічного аналізу визначаються плани розвитку та прогнозуються загрози, це дієвий засіб управління та прийняття рішень.

Економічний аналіз дозволяє, за результатами фінансової діяльності, провести оцінку ефективного застосування активів підприємства. Для таких цілей впроваджений певний ряд показників, що характеризує стан основних і оборотних засобів, активності робочої сили на підприємстві, загальний фінансово-економічний стан підприємства. Аналіз фінансового становища компанії за допомогою відповідних аналітичних методик, показників фінансового стану із застосуванням офіційних документів фінансової звітності компанії. Важливість аналізу прибутковості підприємства зумовлюється тією роллю, яку прибуток відіграє у роботі і розвитку компанії. Фінансовий аналіз проведено на основі звітності підприємства, що опубліковані на сайті підприємства АТ «ХАРТРОН».

Розглянемо техніко-економічні показники результату роботи АТ «ХАРТРОН» за 2019 – 2020рр. (табл.2.1) і зробимо їх порівняльний аналіз.

Таблиця 2.1 – Фінансові результати діяльності АТ «ХАРТРОН»

Стаття	Код	2019		2020	
		тис.грн.	%	тис.грн.	%
1	2	3	4	5	6
Чистий дохід від реалізації	2000	114 593	100	97 024	100
Інші операційні доходи	2120	34 879	30,4	48 751	50,2
Разом доходи		149 472	130,4	145 775	150,2
Матеріальні затрати	2500	37 818	33	31 325	32,3
Витрати на оплату праці	2505	83 500	72,9	72 060	74,3
Відрахування на соціальні заходи	2510	15 847	13,8	14 859	15,3
Амортизація	2515	7791	6,8	7928	8,2
Інші операційні витрати	2520	33 759	29,5	31 773	32,7
Разом операційні витрати	2550	178 381	155,7	151 152	155,8
Чистий прибуток (збиток)	2350 (2355)	7 550	6,6	6 805	7

За результатами аналізу техніко-економічних показників можна відзначити низку негативних змін фінансового становища підприємства. Протягом 2020 року виручка від реалізації зменшилась на 15%, також чистий прибуток зменшився на 10%, із-за зростання витрат зменшення чистого прибутку відбувається повільніше за зменшення виручки від реалізації.

За цими показниками можна прослідкувати негативну динаміку фінансового стану підприємства, але аналіз виявив і деякі позитивні зміни. Наприклад структура виручки стала більш прибутковою: 6,6% у 2019 році, натомість в 2020р. вона становила 7%.

Наступним кроком було розраховано динаміку майнового становища підприємства (табл.2.2).

Таблиця 2.2 – Майнове становище АТ «ХАРТРОН»

Показники	2019		2020		Зміна за рік	
	тис.грн.	%	тис.грн.	%	тис.грн.	частка
1.Необоротні активи	170 027	33,3	131 775	27,8	-38 252	0,77
- інвестиційна нерухомість	29 490	5,8	27 945	5,9	-1 545	0,95
- довгострокові фінансові інвестиції.	40 370	7,9	8 887	1,9	-31 483	0,22
2.Оборотні активи	341 067	66,7	341 247	72,1	180	1
- запаси	210 065	41,1	221 414	46,8	11 349	1,05
- розрахунки з дебіторами	59 135	11,6	35 759	7,5	-23 376	0,6
- грошові кошти	71 867	14,1	84 074	17,8	12 207	1,2
Баланс	511 094	100	473 022	100	-38 072	0,92

Структура майна підприємства майже не змінилася: основну частку складають оборотні активи. Оборотні активи складаються в основному з запасів та грошових коштів.

Також було проаналізовано динаміку активів, результат наведено на рисунку 2.2.

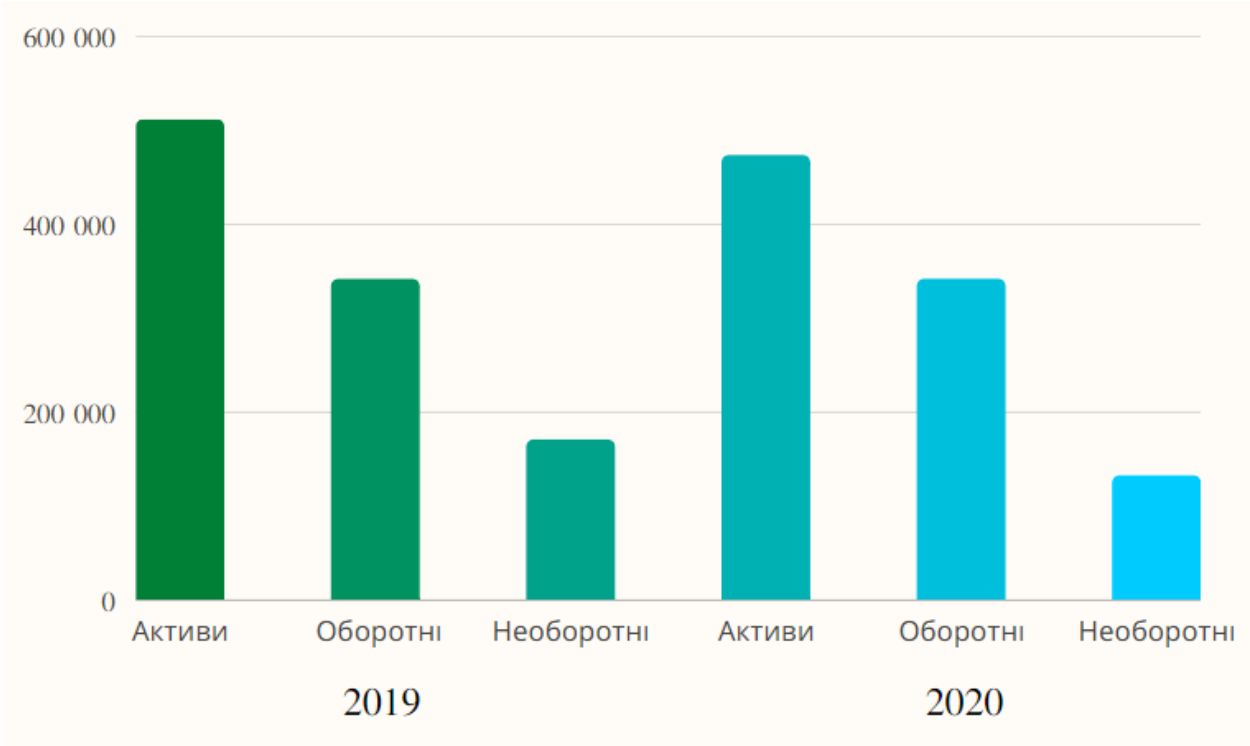

Рисунок 2.2 – Динаміка активів АТ «ХАРТРОН»

За рік спостерігається послаблення господарського потенціалу підприємства, на що вказує зменшення суми активів, це вказує на те, що у підприємства скорочується обсяг наявного у розпорядженні майна. Той факт, що активи скорочуються не так стрімко, як дохід, вказує на необхідність пошуку резервів та термінової оптимізації поточної структури активів.

Зменшення суми балансу зумовлене скороченням переважно необоротних активів, оборотні активи залишаються майже незмінними.

Динаміка джерел фінансування наведена на рисунку 2.3.

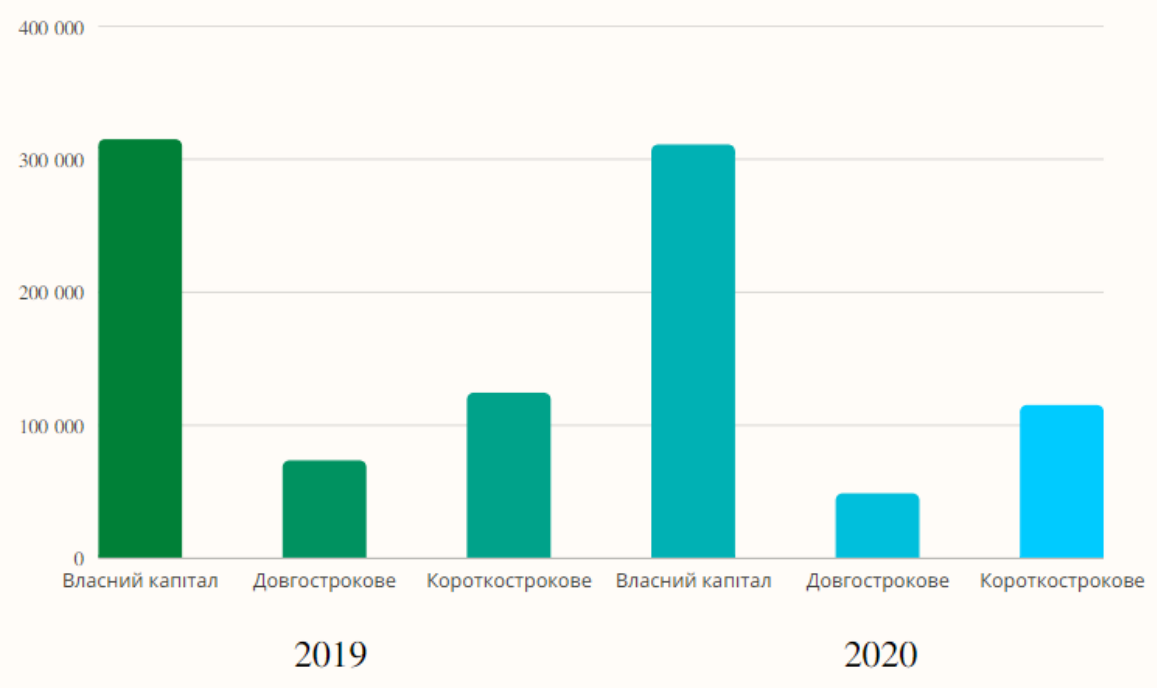

Рисунок 2.3 – Динаміка джерел фінансування АТ «ХАРТРОН»

Скорочується сума наявних джерел фінансування для залучення активів, що зумовлено зменшенням короткострокових зобов'язань підприємства.

Майнове становище АТ «ХАРТРОН» наведено в табл.2.3, 2.4.

Таблиця 2.3 – Майнове становище АТ «ХАРТРОН»

Показник	2019	2020	Абс. приріст, +,-	Відн. приріст, %
Капітал у дооцінках	120 131	150 866	30 735	22,7
Нерозподілений прибуток	127 641	127 231	- 410	-0,32
Власний капітал	314 607	310 592	-4015	-1,28
Довгострокові зобов'язання	72 767	47 968	-24 799	-41,08
Короткострокові зобов'язання	123 720	114 462	-9 258	-7,77
Баланс	511 094	473 022	-38 072	-7,73

Скорочення загальної суми зобов’язань призводить до підвищення незалежності від зовнішніх постачальників фінансових ресурсів, хоча стримує більш повне розкриття наявного потенціалу компанії.

Таблиця 2.4 – Майнове становище АТ «ХАРТРОН»

Показник	2019	2020	Абс. приріст, +,-	Відн. приріст, %
Фінансова автономія	0,62	0,66	0,04	6,25
Поточна ліквідність	4,69	7,11	2,42	41.02

Спостерігається підвищення фінансової незалежності компанії, про що свідчить динаміка коефіцієнта фінансової автономії.

Коефіцієнт автономії (фінансової незалежності) — показує, яку частину у загальних вкладеннях у підприємство складає власний капітал. Він характеризує фінансову незалежність підприємства від зовнішніх джерел фінансування його діяльності. Оптимальне значення більше 0,5.

Коефіцієнт поточної ліквідності (або загальний коефіцієнт покриття боргів, або коефіцієнт покриття, current ratio) характеризує ступінь покриття короткострокових пасивів оборотними активами, і застосовується для оцінки здатності підприємства виконати свої короткострокові зобов'язання. Коефіцієнти ліквідності характеризують платоспроможність підприємства не тільки на даний момент, але й у випадку надзвичайних обставин.

Значення поточної ліквідності знаходиться вище нормативної межі (1,5), що вказує на низьку імовірність втрати платоспроможності у найближчій перспективі.

Динаміка фінансових результатів АТ «ХАРТРОН» наведена на рис. 2.4.

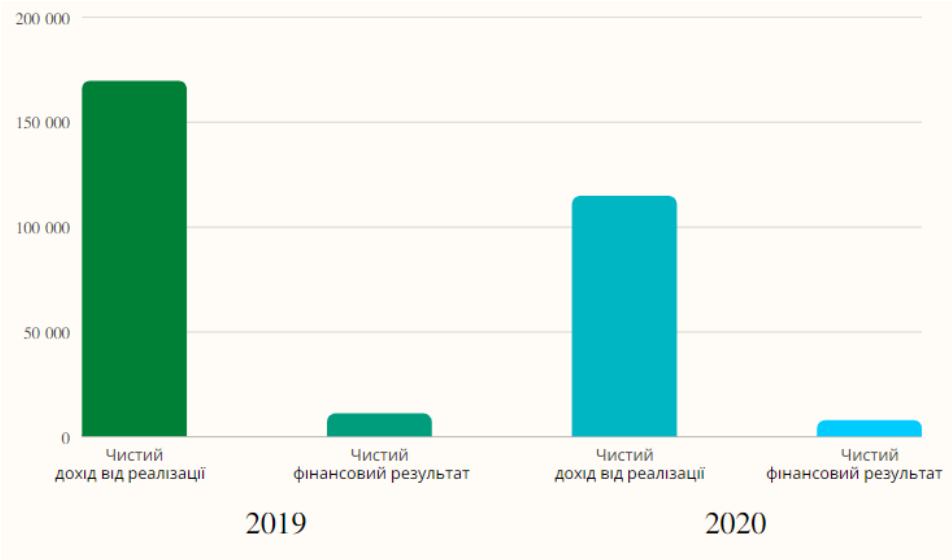

Рисунок 2.4 – Динаміка фінансових результатів АТ «ХАРТРОН»

Зниження чистого доходу від реалізації товарів та послуг вказує на низьку конкурентоспроможність в динамічному середовищі.

Співставлення рентабельності активів АТ «ХАРТРОН» з інфляцією в Україні показано на рис.2.5.

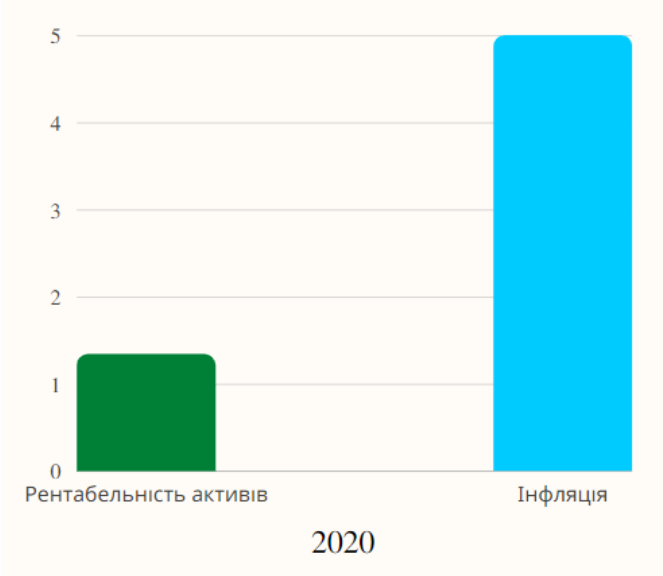

Рисунок 2.5 – Співставлення рентабельності активів АТ «ХАРТРОН» з інфляцією в Україні

Рентабельність активів у 2020р. нижча інфляції, що свідчить про реальне знецінення вартості наявних у компанії активів (рис.2.6).

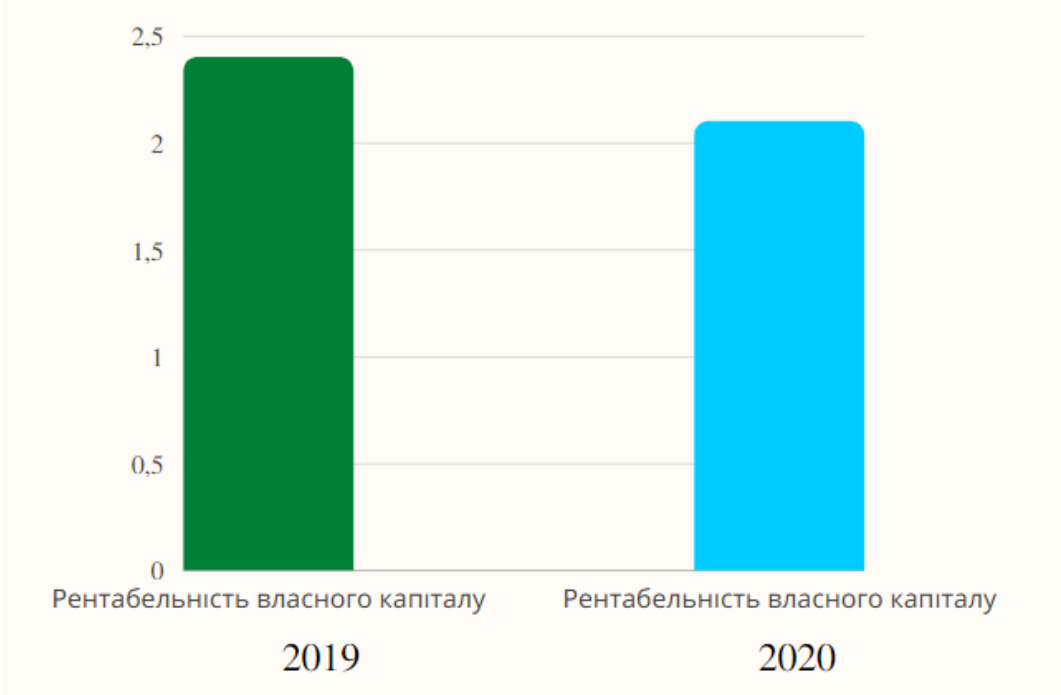

Рисунок 2.6 – Співставлення рентабельності власного капіталу АТ «ХАРТРОН»

Під час функціонування підприємства кількісні величини активів, пасивів, і їх структура постійних змінюються, що можна побачити на таблиці 2.5.

Таблиця 2.5 – Аналіз фінансового балансу АТ «ХАРТРОН»

Стаття	Код	2019		2020	
		тис.грн.	%	тис.грн.	%
АКТИВИ					
I. Необоротні активи					
Нематеріальні активи	1000	5 504	1	4 229	0,9
- первісна вартість	1001	5 504	1	4 229	0,9
Основні засоби:	1010	45 587	8,9	40 903	8,6
- первісна вартість	1011	45 587	8,9	40 903	8,6

Продовження таблиці 2.5

Інвестиційна нерухомість	1015	29 490	5,8	27 945	5,9
Довгострокові фінансові інвестиції	1030	40 370	7,9	8 887	1,9
Інші фінансові інвестиції	1035	49 076	9,6	49 811	10,5
Усього за розділом I	1095	170 027	33,3	131 775	27,8
II. Оборотні активи					
Запаси	1100	210 065	41,1	221 414	46,8
Дебіторська заборгованість за товари	1125	35 066	6,9	21 901	4,6
Інша поточна дебіт. заборгованість	1155	24 069	4,7	13 858	2,9
Гроші та їх еквіваленти	1165	71 867	14	84 074	17,8
Усього за розділом II	1195	341 067	66,7	341 247	72,1
Баланс	1300	511 094	100	473 022	100
ПАСИВИ					
I. Власний капітал					
Зареєстрований капітал	1400	21 368	4,2	21 368	4,5
Капітал у дооцінках	1405	120 131	23,5	150 866	31,9
Резервний капітал	1415	21 670	4,2	5 342	1,1
Нерозподілений прибуток (збиток)	1420	127 641	25	127 231	26,9
Неконтрольована частка	1490	23 797	4,6	5 785	1,2
Усього за розділом I	1495	314 607	61,5	310 592	65,7
II. Довгострокові зобов’язання і забезпечення:					
Довгострокові забезпечення	1520	72 767	14,2	47 968	10,1
Усього за розділом II	1595	72 767	14,2	47 968	10,1
III. Поточні зобов’язання					
Короткострокові кредити банків	1600	4 000	0,8	4 950	1
Кредит. заборгованість за товари	1615	103 501	20,2	86 989	18,4
Поточні забезпечення	1660	7 089	1,4	8 932	1,9
Інші поточні зобов'язання	1690	9 130	1,8	13 591	2,9
Усього за розділом III	1695	123 720	24,2	114 462	24,2
Баланс	1900	511 094	100	473 022	100

Розрахунок фінансових показників діяльності відображає стан розвитку підприємства, його можна розбити на чотири групи: показники ліквідності, показники фінансової стійкості, показники рентабельності показники оборотності.

Ліквідність – це рухливість активів підприємства, яка дозволяє вчасно оплачувати фінансові зобов'язання.

Показники ліквідності характеризують здатність підприємства покривати свої короткострокові зобов'язання оборотними засобами. Але оскільки оборотні засоби є неоднорідними, вони мають різну ліквідність, тому визначають ліквідність окремо для кожної групи через різні показники.

Розглянемо 4 базові показники ліквідності (табл.2.6)

Таблиця 2.6 – Показники ліквідності АТ «ХАРТРОН»

Показник	Норма	2019	2020
Поточна ліквідність	від 1 до 2,5	2,7	2,9
Термінова ліквідність	більше 1,0	0,99	1,05
Абсолютна ліквідність	від 0,2 до 0,5	0,58	0,73

Фінансова стійкість характеризує, наскільки ефективно співвідносяться пасиви та активи. Тобто, з яких джерел фінансується бізнес – зі своїх чи з чужих. У процесі діяльності йде постійна взаємодія пасивів та активів:

- за рахунок пасивів фінансується купівля активів;
- за рахунок активів поповнюються пасиви.

Чим більше позикових коштів використовує підприємство, тим більше воно залежить від зовнішніх джерел фінансування. І це означає втрату фінансової стійкості (автономності) (табл. 2.7).

Таблиця 2.7 – Показники фінансової стійкості АТ «ХАРТРОН»

Показники	Норма	2019	2020
Коефіцієнт фінансової автономії	>0,5	0,61	0,66
Коефіцієнт фінансової залежності (левериджу)	<1	0,62	0,52
Коефіцієнт маневреності	>0	0,69	0,73

Показники рентабельності показують співвідношення доходів та витрат бізнесу в процесі виробництва та реалізації. У загальному випадку рентабельність – відношення суми доходів до витрат за їх (її) отримання (табл. 2.8).

Таблиця 2.8 – Показники рентабельності АТ «ХАРТРОН»

Показник	2019	2020
Прибутковість виробництва	0,22	0,26
Прибутковість продажів	0,060	0,109
Доходність активів	0,014	0,014
Доходність власного капіталу	0,023	0,021

Показники ділової (фінансової) активності характеризують швидкість, з якою гроші, вкладені у бізнес, повертаються (табл.2.9).

Таблиця 2.9 – Показники ділової активності АТ «ХАРТРОН»

Показник	2019	2020
Оборотність активів	0,224	0,205
Час обороту, днів	4,4 роки	4,8 роки

Показники ліквідності характеризують можливість підприємства покривати свої короткострокові обов’язки оборотними активами. Так як оборотні активи неоднорідні, вони мають різну ліквідність. Тому ліквідність визначають окремо по кожній з груп через різні показники. Коефіцієнт

покриття знаходиться в нормі. Коефіцієнт термінової ліквідності знаходиться в значенні менше норми в 2019 році, але в 2020 знаходиться в нормальних значеннях, коефіцієнт абсолютної ліквідності також не виходить за межі норми.

Показники фінансової стійкості показують ефективність співвідношення пасивів та активів. Коефіцієнт левериджу і коефіцієнт маневреності знаходиться в нормі і в 2019, і в 2020 роках, а коефіцієнт автономії перевищує свої нормальні значення.

Показники прибутковості й доходності виражають співвідношення доходів і витрат фірми в процесі виробництва і реалізації. В загальному випадку рентабельність – відношення суми доходів до витрат на їх отримання. Можна виділити дві групи рентабельностей. Показники цієї групи розраховані успішно і знаходяться в допустимих значеннях.

Показники ділової активності характеризують швидкість, з якою гроші, вкладені в бізнес, повертаються. При розрахунку цих показників стало зрозуміло, що оборотність активів підкріплюється падаючим коефіцієнтом, що говорить про від’ємні тенденції, так само як і коефіцієнт часу обороту демонструє від’ємну тенденцію.

2.3 Аналіз існуючих підходів до організації системи інформаційної безпеки підприємства АТ «ХАРТРОН»

Враховуючи те, що підприємство АТ «ХАРТРОН» займається розробкою різноманітних систем управління для ракетних комплексів та космічних апаратів, також автоматизованих систем управління та систем діагностики, відповідає за виготовлення апаратури систем управління ракетних комплексів та космічних апаратів також різноманітних

комп’ютерних системи, можна зазначити, що інформаційний захист на рівні цифрових та аналогових засобів реалізації інформаційної безпеки мереж передачі даних, баз даних, інших засобів передачі даних реалізована на достатньому рівні. Досвід у розробці телеметричної апаратури та волоконно-оптичних ліній зв'язку дозволяють підприємству реалізовувати максимально безпечні шляхи передачі даних між відповідними кадрами.

АТ «ХАРТРОН» було найбільшим у СРСР розробником і виробником систем керування ракет стратегічного призначення та космічних апаратів, це посприяло високому рівню конфіденційної інформації, а також потреби в її захисті.

Служби з кадрів забезпечують підприємство безпекою в питаннях доступу робітників до інформації, підписання договорів про нерозголошення, програми навчання та інформування персоналу щодо особистих рішень інформаційної безпеки. Служби з роботи з інтернет ресурсами забезпечують безпечні реалізації зберігання та передачі інформації через локальні та глобальні мережі, відповідні системи автентифікації користувачів та рівні доступу до інформації. Також реалізують діяльність з протидії віддаленим інтернет атакам та можливим загрозам фішингу, передачі вірусів або інтернет шахрайства. Відповідні відділи контролю відповідають за регулярну перевірку дотримання норм безпеки персоналом.

За напрями діяльності АТ «ХАРТРОН» активно займається як системним аналізом і пошуком адміністративно-організаційних рішень, в тому числі для питань інформаційної безпеки, так і реалізацією апаратних рішень науково технічного характеру. Активна залученість в сферу інформаційних технологій зумовлює потребу в реалізації потужних систем інформаційної безпеки, як програмного характеру так апаратного і організаційного. Великий досвід в математичному моделювання процесів керування та технологічних процесів дозволяє підприємству проводити

аналіз та моделювання потенційних загроз та заздалегідь визначати стратегії протидії.

Таким чином було проаналізовано діяльність та управління інформаційною безпекою підприємства АТ «ХАРТРОН», надана характеристика діяльності та контуру управління підприємства, проведено аналіз економічних та фінансових показників діяльності, визначено існуючі підходи до організації системи інформаційної безпеки підприємства. В результаті дослідження було зроблено висновок, що підприємство АТ «ХАРТРОН» характеризується негативним розвитком, як фінансовим так і виробничим. Присутній попит на послуги підприємства та наявність елементів безпеки інформаційного середовища підприємства, фінансова стійкість бізнес-моделі адаптується до сучасних умов, таким чином підприємство продовжує розвивати перспективні напрями.

3 УДОСКОНАЛЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

3.1 Напрямки удосконалення системи інформаційної безпеки в умовах гібридних загроз

Підприємства регулярно стикаються з проблемами забезпечення інформаційної безпеки. Це зумовлено завданнями забезпечення функціонування та стабільністю досягнення результатів підприємницької діяльності в умовах невизначеного та нестабільного середовища. Загалом інформаційна безпека підприємства – це складна організаційна структура, метою якої є ефективне використання наявних ресурсів, задля запобігання можливим інформаційним загрозам і створення сприятливих умов стабільного функціонування та розвитку усіх підрозділів підприємства. Підрозділи, які відповідають за протидію гібридним загрозам визначають нестабільні ризики та впроваджують рішення з протидії [38-39].

Важливим фактором ризику є проблема з реалізацією загального, офіційного та швидкого обміну інформацією щодо потенційних загроз між державними та недержавними підприємствами. Проблемою також виступає високий рівень інтеграції інформаційного середовища, зважаючи, що політика безпеки держави залишається орієнтованою на національний масштаб. Ще один можливий ризик пов’язаний з високою цифровізацією діяльності підприємства, що з одного боку забезпечує зручну та швидку реакцію на операційну діяльність підприємства, з іншого боку створює потребу в організації якісного кіберзахисту та протидії загроз пов’язаних з використанням інформаційних технологій. Великі обсяги фінансових операцій та бізнес-процесів підприємств реалізується у цифрових системах збереження та обміну інформації, це збільшує ефективність, але і підвищує вразливість систем до кібератак, вірусів, фішингу, тощо. Це зумовлює важливість використання систем автентифікації та визначення доступу до

інформації та робить взаємодію з інформаційними структурами ефективним засобом для противника у способах гібридного вплив. Тож можна зазначити, що кібербезпека, питання доступу до інформації, програмні засоби захисту систем стають важливим напрямком вдосконалення системи інформаційної безпеки. Напрямок впровадження програмного забезпечення реалізується за допомогою таких засобів, як антивірусні програми, які перевіряють комп'ютер на наявність шкідливих програм, використання хмарних систем також допомагає захищати дані від вірусів, впровадження програмних систем аналізу вхідної та вихідної інформації, систем шифрування даних, які реалізують безпечну передачу даних та роблять майже неможливим її перехоплення. Важливою є і реалізація захисту фізичних дротових мереж сучасними методами та протоколами захисту, також захист доступу до глобальних мереж. Наприклад, використання міжмережевого екрану для блокування та фільтрації трафіку, або SIEM моніторинг, який фіксує та зберігає логи, аналізує та виявляє шкідливих дії.

Відсутність активної координації та комунікації між підприємствами для протидії гібридним загрозам нівелює рівень захисту, який може суттєво відрізняться. Це велика проблема, бо складність виявлення гібридних загроз залежить від того, як гібридні загрози проявляються, вони можуть надсилати лише слабкі сигнали, які дуже важко виявляти окремим підприємствам. Напрямок організації комунікативних шляхів різних підприємств може полегшити виявлення загроз та зробити протидію їм більш комплексною, за рахунок залучання можливостей різного масштабу систем протидії загрозам різних підприємств. Таким чином інформаційні системи підприємств потребують нових комплексних рішень для попередження про гібридні загрози [40].

3.2 Розробка системи інформаційної безпеки підприємства в умовах гібридних загроз

В умовах гібридних загроз інформаційна безпека представляє набір інструментів та методів для захисту різних видів інформації та реагування на виникнення нових загроз у стані невизначеності. Вона включає безліч сучасних інформаційних технологій, використання яких стає необхідністю успішного функціонування підприємства. Під інформаційною безпекою розуміється стан інформаційного середовища, який забезпечує розвиток цього середовища, ефективне використання інформації в інтересах підприємства, а також захищеність від будь-яких загроз та спроможність реагувати та змінюватись в залежності від внутрішніх і зовнішніх факторів, задля забезпечення безпечної діяльності підприємства. Забезпечення інформаційної безпеки на підприємстві слід розглядати як невід'ємний елемент процесу управління підприємством, в контексті існування гібридних загроз, невдале керування підприємством ставить під сумнів безпекові характеристики підприємства [41-42].

Застосування СУІБ (Система управління інформаційною безпекою) є однією з умов активного розвитку бізнесу, її використання при виникненні гібридних загроз інформаційним системам підприємства забезпечує спроможність до попереднього виявлення, протистояння загрозі та подальшого існування. Використання методів ризик-менеджменту, а також застосування інших технічних та організаційних процедур, методів, програмного та технічного забезпечення, зумовлює досягнення реалізації інформаційної безпеки підприємства спроможної протистояти гібридним загрозам. Реалізація системи управління інформаційною безпекою може бути організовано як дерево процесів. Створення ефективної системи управління інформаційною безпекою можна описати певною послідовністю заходів на підприємстві, така послідовність може включати етапи, які наведені на рисунку 3.1.

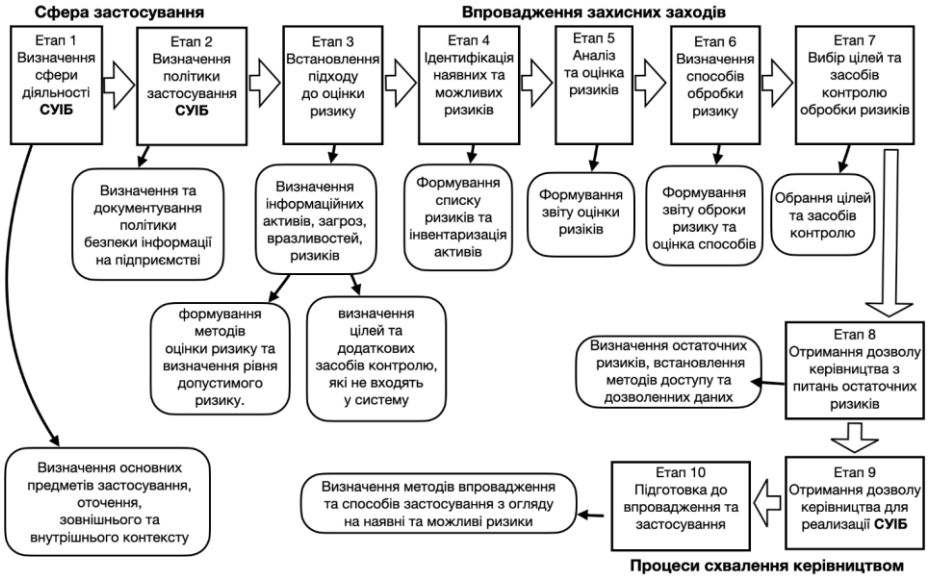

Рисунок 3.1 – Послідовність формування системи управління інформаційною безпекою на підприємстві

Фактична реалізація етапів формування системи управління інформаційною безпекою залежить від специфіки конкретного підприємства. Етапи формування визначають впровадження відповідних заходів, виконання дій або прийняття рішень, які можна поділити на три блоки. Перший та другий етап забезпечують встановлення сфери застосування СУІБ. З третього по сьомий етапи відбувається впровадження захисних заходів на основі ризик-менеджменту. Етапи 8-10 зазначають процеси схвалення керівництвом рішень для впровадження засобів обробки ризиків, формулювання вимог, та дозволів на реалізацію та використання механізмів системи.

Враховуючи велику кількість процесів інформаційної безпеки під час діяльності підприємства, ефективна СУІБ повинна враховувати засоби призначені для розробки, впровадження, функціонування, моніторингу, перегляду, підтримування, а також розвитку та вдосконалення інформаційної безпеки. Також важливо враховувати вже напрацьовані стандарти, які допоможуть реалізувати ефективну у використанні систему, такі стандарти, пропонують сформовані вимоги до побудови, методи використання та засоби розвитку СУІБ на підприємстві.

Таким чином системи управління інформаційною безпекою є невід’ємною частиною загального управління підприємством, вони

забезпечують стійкість інформаційних структур до внутрішніх та зовнішніх загроз а також дозволяють впроваджувати заходи щодо розвитку, завдяки можливості прогнозувати стан підприємства відносно можливих загроз. Великий досвід застосування міжнародних стандартів формування систем управління інформаційною безпекою підприємства, який базується на основі менеджменту ризиків, дозволяє будувати системи, які спроможні захищати підприємство та забезпечувати його розвиток. Треба також зазначити, що під час реалізації інформаційної безпеки перед підприємством постає задача у пошуку ефективного балансу між відповідністю системи та її засобів конкретному підприємству, зручністю використання та рівнем забезпечення безпеки інформації [43-44].

3.3 Удосконалення системи інформаційної безпеки підприємства АТ «ХАРТРОН»

Удосконалення механізму захисту та системи інформаційної безпеки підприємства АТ «ХАРТРОН» в умовах гібридних загроз базується на аналізі існуючої системи забезпечення інформаційної безпеки, оскільки розвиток системи розвиває та додає нові спроможності, або змінює існуючу систему захисту та протидії інформаційним загрозам. Одним з шляхів може бути реалізація загальної системи обміну інформацією щодо потенційних загроз між АТ «ХАРТРОН» та іншими підприємствами, це може посприяти рівню захищеності інформаційної системи. Проблемою також висткпає високий рівень інтеграції інформаційного середовища підприємства з державним, що поширює джерела загроз, так само як і діяльність підприємства у оборонно-промислових проектах.

Виходячи з об’єктів розробки АТ «ХАРТРОН», які здебільшого складають проекти цифрового характеру, можна зазначити, що великим ризиком є і високий рівень цифровізації діяльності, що створює потребу в

організації якісного кіберзахисту та протидії загроз пов’язаних з використанням інформаційних технологій. На підприємстві АТ «ХАРТРОН» існує потреба в безперервному розвитку автентифікації та визначення доступу та допуску до інформації, яка може бути комерційною таємницею. Важливою є і реалізація захисту технічних засобів, як дротових мереж так і серверів, виробничих засобів програмного забезпечення сучасними методами та протоколами захисту, також захист доступу до глобальних мереж та використання міжмережевого захисту, задля запобігання доступу до внутрішньої інформації підприємства.

Складність виявлення гібридних загроз становить важливий вектор удосконалення спроможностей АТ «ХАРТРОН» до спостереження за загрозами, в залежності залежить від того, як гібридні загрози проявляються, вони можуть дуже важко виявлятись окремим підприємством, тому існує потреба у співробітництві з державними структурами та іншими підприємствами з метою посилення рівня обізнаності потенційних загроз. Організація комунікативних шляхів між підприємствами може полегшити процес виявлення загроз, пришвидшити реакцію на них та зробити протидію їм більш комплексною, за рахунок залучання можливостей різного масштабу систем протидії загрозам різних підприємств. Невеликі компанії також можуть стати інструментом гібридних загроз, шпіонське програмне забезпечення залучає мільйони комп'ютерів для скоєння DOS-атак, якщо скоординовані гібридні атаки виконуються одночасно через різні частини інфраструктури, підприємство може отримати руйнівний ефект [45].

Не зважаючи на те, що АТ «ХАРТРОН» підприємство доволі великого масштабу воно все одно не має можливостей держави. Тому слід зосередитись на зменшенні вразливості та підвищенні стійкості. Побудова резервних інформаційних систем та виконання регулярних бекапів в критичних для бізнесу сферах, удосконалення системи кіберзахисту, навчання персоналу особистим методикам протидії про гібридні загрози, обмін інформацією між підприємствами взаємодія з національними безпековими організаціями. Важливим є регулярне тестування системи

безпеки, воно реалізується моделюванням реальних атак різного характеру з метою перевірити стійкість системи. Такі рекомендації створені для того, щоб доповнювати та посилювати наявні механізми забезпечення безпеки, інтегруючись в них та не порушуючи бізнес-діяльність [46].

За допомогою створення в рамках підприємства нормативно-правових актів та підписання договорів про нерозголошення, правила користування та передачі отриманої інформації з співробітниками можна посилити безпеку розповсюдження інформації персоналом, та захистити підприємство від злочинного впливу людського фактору. Важливим є і впровадження в структурі АТ «ХАРТРОН» відповідного контролю за виконанням усіх внутрішніх нормативних документів та впровадження системи автентифікації та відповідних рівнів доступу до інформації різних ступенів секретності, задля уникнення зайвого витоку конфіденційної інформації. Впровадження механізмів оцінки працездатності та ефективності роботи системи управління інформаційною безпекою підприємства та своєчасний розвиток системи за результатами регулярних оцінок загроз.

Для забезпечення комплексного підходу система захисту бізнесу в умовах гібридних загроз має доповнюватись такими структурними елементами, як принципи керування роботи компанії в умовах гібридних загроз, спроектовані моделі для захисту даних, інформації та працівників, екстрений план безперервності роботи в умовах дефіциту важливих ресурсів, програми навчання та інформування персоналу, механізми та шляхи обміну безпековою інформацією між компаніями, механізми співпраці підприємства з владою та службами безпеки для створення комплексної платформи з протидії гібридним загрозам.

Важливою характеристикою інформаційних загроз є її приховані здатності, спроможності для злочинної діяльності, що можуть проявлятися за певних умов, та бути непомітними за звичайних умов, таким чином існує потреба у резервних системах. Створення резервних систем є важливим напрямком посилення інформаційної безпеки, також він розглядається як обов'язковий елемент в системах захисту критичної інфраструктури

підприємства, особливо в умовах гібридних загроз важливість цього неймовірно актуалізується [47-48].

Існуюча система інформаційної безпеки АТ «ХАРТРОН» є достатньо опрацьованою та містить базові елементи захисту від зламу на основі прийнятого на підприємстві Протоколу організаційного захисту.

Цей документ визначає регламентацію виробничої діяльності і взаємин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне заволодіння конфіденційною інформацією. Інформаційну безпеку забезпечують такі елементи організаційного захисту:

- організація охорони, режиму, роботу з кадрами, з документами;
- використання технічних та програмних засобів безпеки.

АТ «ХАРТРОН» вживає низку організаційних заходів, які створюють захист в сфері ІТ. Для запобігання раптових перебоїв в роботі підприємству була запропонована низка додаткових заходів, які підвищують стійкість процесів та підвищують інформаційну безпеку (табл.3.1).

Таблиця 3.1 – Організаційні заходи ТОВ АТ «ХАРТРОН», які створюють захист в сфері інформаційної безпеки

Тип захисту	Існують на підприємстві	Запропоновані
Організаційні заходи	- організація режиму і охорони для виключення можливості таємного проникнення сторонніх осіб; - організація роботи зі співробітниками (ознайомлення з заходами відповідальності тощо); - організація роботи з документами.	- організація роботи зі співробітниками (навчання правилам роботи з інформацією в умовах гібридних загроз за рекомендаціями WARN-проєкту [49]); - організація використання технічних засобів.
Засоби захисту від несанкціонованого доступу	- засоби авторизації; - мандатне управління доступом.	- журналювання (резервна система)
Системи аналізу інформаційних потоків.	відсутні	- системи аналізу інформаційних потоків (CASE-системи)

Продовження таблиці 3.1

Системи моніторингу мереж	- системи запобігання витоків конфіденційної інформації (DLP-системи).	- системи виявлення й запобігання вторгнень (IDS / IPS).
Тип захисту	Існують на підприємстві	Запропоновані
Криптографічні засоби	- шифрування; - цифровий підпис.	Не запропоновано
Системи резервування	відсутнє	- резервне копіювання (резервна система)
Системи безперебійного живлення	- джерела безперебійного живлення	Резервна система: - резервні лінії електроживлення; - генератори електроживлення.
Системи аутентифікації на основі	- пароля	- електронного ключа доступу

Більшість із запропонованих заходів спрямована на отримання додаткових резервів або процесів, які захищають вразливі елементи бізнесу від нападу, тобто коли бізнес є об'єктом атаки. Але ж використання бізнесу в гібридних впливах може мати на меті перетворення такого бізнесу на засіб атаки (або на один з багатьох засобів). Тому саме для бізнесу такі впливи не представляють загрози, але для громади, суспільства, оточуючого середовища це може мати руйнівний характер. Руйнуючи оточуюче середовище, бізнес руйнує й власні перспективи не тільки розвитку, але й існування.

Тому для АТ «ХАРТРОН» була запропонована низка індикаторів, яка відстежує несанкціоновані слабо помітні дії в інформаційному середовищі– табл.3.2. Такий підхід був запропонований саме для моніторингу бізнесу в умовах гібридних загроз [50].

В результаті проведеного моніторингу було виявлене незначне гальмування як часу проведення як внутрішніх операцій, так й зовнішніх.

Результати стали підставою для запиту на проведення аудиту з боку партнерів.

Таблиця 3.2 – Система індикаторів слабких сигналів інформаційної безпеки АТ «ХАРТРОН»

№	Індикатор	Сутність	Од. вим.	Порогове значення	
				показника	інтенсивності
1	Гальмування власне	затримка швидкості типової операції	%	10	Більш ніж 250
2	Трафік	Необґрунтована зміна трафіку	%	25	Більш, ніж 3 – менш ніж 17 разів за місяць
3	Чорні списки	Потрапляння у ворожу банерну систему	так чи ні	Так (факт виявлення)	1 (з першого разу)
4	Автопілот-IT	Перехоплення управління скриптами	так чи ні	Так (факт виявлення)	1 (з першого разу)
5	Автопілот-менеджмент	Перехоплення управління папками адміністратора – зараження локальної мережі	так чи ні	Так (факт виявлення)	1 (з першого разу)
6	Троянський кінь	Контроль IP партнерів (при запиті власний сайт зависає)	так чи ні	Так (факт)	1 (з першого разу)
7	Гальмування стороннє	Зростання часу видачі API від партнера	%	100	Більше 5 разів

Підприємство в своїй практиці стикалось із недружніми впливами, пов'язаними із кібератаками на сайт. Але щодо гібридних загроз – такі загрози не розглядались керівництвом як актуальні загрози бізнесу та не досліджувались.

Таким чином, підприємство АТ «ХАРТРОН», що працює в таких сегментах ринку, як ракетно-космічна галузь, енергетика, в тому числі атомна, залізничний транспорт, є потенційним об'єктом ворожив впливів.

Запропоновані підходи дозволяють посилити захист підприємства в умовах гібридних впливів через посилення системи інформаційної безпеки.

В результаті визначені шляхи удосконалення системи інформаційної безпеки та запропоновані практичні рекомендації. Запропоновані методи удосконалення системи інформаційної безпеки підприємства АТ «ХАРТРОН», запропонована низка індикаторів, яка відстежує несанкціоновані слабо помітні дії в інформаційному середовищі. Запропоновані підходи дозволяють посилити захист підприємства в умовах гібридних впливів через посилення системи інформаційної безпеки.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було досліджено поняття системи інформаційної безпеки підприємства в умовах гібридних загроз та проаналізовано методи забезпечення інформаційної безпеки. Також було досліджено та сформовано теоретичні матеріали та розроблені практичні рекомендації з побудови системи інформаційної безпеки підприємства в умовах гібридних загроз.

У першому розділі роботи розглянуто теоретичні основи формування інформаційної безпеки підприємств та потенційні можливі гібридні загрози та їх вплив на інформаційну складову безпеки. Також розглянуті засоби захисту інформаційного середовища підприємств в умовах гібридних загроз, розкритий актуальний стан гібридних впливів на інформаційні системи та описана важливість стійкості до гібридних загроз як складової інформаційної безпеки підприємств. Проведений аналіз існуючих підходів до рішення проблем та питань забезпечення інформаційної безпеки в сучасному безпековому ландшафті та умовах гібридних загроз. До того ж визначений вплив інформаційної безпеки на якість роботи підприємств та більш широко розкрите поняття гібридних загроз та їх впливу.

В другому розділі проаналізовано діяльність та управління інформаційною безпекою підприємства АТ «ХАРТРОН», надана характеристика діяльності та контуру управління підприємства, проведено аналіз економічних та фінансових показників діяльності, визначено існуючі підходи до організації системи інформаційної безпеки підприємства. В результаті дослідження було зроблено висновок, що підприємство АТ «ХАРТРОН» працює в ракетно-космічній галузі, енергетиці, залізничному транспорті, діяльність характеризується негативним розвитком, як фінансовим так і виробничим. Присутній попит на послуги підприємства та

наявність безпекових елементів захисту як інформаційного так і бізнес середовища підприємства, фінансова стійкість бізнес-моделі адаптується до сучасних умов, таким чином підприємство продовжує активно розвивати перспективні напрями.

В третьому розділі визначені шляхи удосконалення системи інформаційної безпеки підприємства в умовах гібридних загроз та запропоновані практичні рекомендації до розробки системи інформаційної безпеки підприємства. Запропоновані методи удосконалення системи інформаційної безпеки підприємства АТ «ХАРТРОН», запропонована низка індикаторів, яка відстежує несанкціоновані слабо помітні дії в інформаційному середовищі, такий підхід був запропонований саме для моніторингу бізнесу в умовах гібридних загроз. Запропоновані підходи дозволяють посилити захист підприємства в умовах гібридних впливів через посилення системи інформаційної безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. №5. С.55-65.

2. Колобчинський О.Л. Методика формування системи економічної безпеки підприємства. *Актуальні проблеми економіки*. 2009. № 4(94). С. 41-45.

3. Кавун С.В. Жизненный цикл системы экономической безопасности предприятия. *Управління розвитком*. 2008. № 6, С. 17-21.

4. Соколова Л.В., Шутов К.В. Информационное обеспечение функционирования комплексной системы экономической безопасности предприятия. *Управління розвитком*. 2008. № 14, С. 18-19.

5. Орлов П.І., Духов В.Є. Основи економічної безпеки фірми: Навчальний посібник. Х.:ТОВ «Прометей-Прес», 2004. 284 с.

6. Економічна безпека підприємств: підручник . В.Л. Ортинський, І.С. Керницький, З.Б. Живко та ін. К.: Алерта, 2011. 704 с.

7. Головченко О. М. Економічна безпека регіону в гарантуванні стабільності національної економіки: Монографія. Одеса, 2008. 399 с.

8. Грішин С.П., Зубарев О.В., Коротков В.Ю. Основні складові та напрямки забезпечення економічної безпеки підприємства. *Інформаційна безпека.* 2009. № 2 (2). С. 84–88.

9. Передерій Л.В. Системний підхід до захисту інформації в автоматизованих системах. *Науковий вісник Донбасу*, 2010. № 2. URL: http://nbuv.gov.ua/UJRN/nvd_2010_2_7

10. Катренко А.В. Системний аналіз об’єктів та процесів комп’ютеризації. Навчальний посібник. Львів: Новий світ-2000, 2003. 424 с.

11. Живко З.Б. Системний підхід до управлінського процесу підприємства: інформаційні технології та взаємодія підсистем безпеки.

Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна. 2013. Випуск 1. С. 230-237.

12. Козаченко Г.В., Пономарьов В.П., Ляшенко О.М. Економічна безпека підприємства: сутність та механізм забезпечення: монографія. К.: Лібра, 2003. 280 с.

13. Користін О. Є., Барановський О.І., Герасименко Л.В. Економічна безпека: навч. посіб. К.: КНУВС, 2010. 368 с.

14. Живко З.Б., Баворовська О.Б., Живко М.О. Менеджмент безпеки персоналу: навч. посіб. Львів: Ліга-Прес, 2011. 228 с.

15. Гбур З.В. Актуальні гібридні загрози економічній безпеці України. *Інвестиції: практика та досвід*. 2018. № 7. С. 97-99.

16. Ліпкан В.А. Сутність гібридної війни проти України. *Глобальна організація союзницького лідерства.* 2015. URL: http://goal-int.org/sutnist-gibridnoi-vijniproti-ukraini/

17. Магда Є. Гібридна війна: питання і відповіді. *Media Sapiens.* 2015. URL: http://ms.detector.media/rends/1411978127/gibridna_ viyna_ pitannya_i_ vidpovidi/

18. Магда Є.М. Гібридна війна: сутність і структура феномену. *Міжнародні відносини: Серія "Політичні науки".* 2014. № 4. С.216-226.

19. Мальський М.З., Кучик О.С., Вовк Р.В. Транскордонна безпека: політико-правовий, соціально економічний, гуманітарний та екологічний вимір. *Збірник матеріалів Міжнародної науково практичної конференції*, Львів, 21 квітня 2017 року, Львів: Факультет міжнародних відносин, 2017. 96 с.

20. Мартинюк В. Гібридні загрози Україні і суспіль на безпека. Досвід ЄС і східного партнерства. Київ, 2018. 106 с.

21. Предборський В.А. «Гібридна» війна як відбиття закономірностей розвитку суспільства незавершеної модернізації. *Формування ринкових відносин в Україні.* 2014. № 10. С. 13-18.

22. On cyber threats at Davos. URL: http://bit.ly/2V5cbj9. [Accessed: 17 February 2020]

23. Борсуковський Ю.В. Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. *Кібербезпека: освіта, наука, техніка.* 2019. № 1. С. 61-72. URL: http://nbuv.gov.ua/UJRN/cest_2019_1_8

24. Івченко Є. А. Трансформації системи економічної безпеки підприємства: монографія. Сєвєродонецьк: вид-во СНУ ім. В. Даля, 2018. 420 с.

25. Козаченко Г. В., Погорелов Ю. С. Про деякі проблеми у сучасній економічній безпекології. *Управління проектами та розвиток виробництва*: зб. наук. праць. Луганськ (Сєвєродонецьк): Вид-во СНУ ім. В. Даля, 2015. Вип. 3(55). С. 6–18.

26. Пазєєва Г. М. Комплексна діагностика в забезпеченні економічної безпеки підприємств (на матеріалах транспортно-експедиційних підприємств України): дис. канд. екон. наук: 21.04.02. Київ, 2017. 300 с.

27. Янковець Т. М. Взаємозв'язок потенціалу, економічної безпеки та розвитку економічних систем. *Актуальні проблеми економіки*. 2015. № 9. С. 66-73.

28. Алькема В. Г. Потенціал системи економічної безпеки транспортно-експедиційного підприємства. *Управління проектами та розвиток виробництва*. 2015. № 3. С. 43-60.

29. Гладишенко М. І. Правові та організаційні аспекти діяльності підприємця для захисту комерційної таємниці. *Персонал*. 2005. № 3. С. 51-55.

30. Андрощук Г., Крайнев П.П. Економічна безпека підприємства: Захист комерційної таємниці. К.: Вид. дім «Ін Юре», 2000. 398 с.

31. Недержавна система безпеки підприємництва як складова національної безпеки України. Зб. наук. праць. К.: Європейський ун-т, 2004. 338 с.

32. The landscape of Hybrid Threats: A Conceptual Model (Public Version). Giannopoulos, G., Smith, H. and Theocharidou, M. (ed.). EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021. 58 p.

33. Smith H. Power of the powerful or power of the “weak”? Hybrid Centre of Excellence Hybrid CoE Strategic Analysis. Finland: Hybrid CoE, 2017. 8 p.

34. Гришко С,. Кодрул Р. Зміна безпекового ландшафту як передумова розвитку гібридних загроз: матеріали *Міжнародної науково практичної конференції «Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці»*, м.Київ, 22 листоп. 2022 р. С.324-334.

35. Нехай В.В., Нехай В.А. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент.* 2017. - Вип. 24(2). С. 137-140. URL: http://nbuv.gov.ua/UJRN/Nvmgu_eim_ 2017_24%282%29__30

36. Козаченко Г.В., Пономарьов В.П., Ляшенко О.М. Економічна безпека підприємства: сутність та механізм забезпечення: монографія. К.: Лібра, 2003. 280 с.

37. Статут акціонерного товариства «ХАРТРОН» (нова редакція) (код ЄДРПОУ 14313062) % м. Харків •. 2019.

38. Живко З. Економічна безпека підприємств, організацій, установ. К.: «Правова єдність», 2009. 544 с.

39. Салоїд С. Механізм управління економічною безпекою підприємства: теоретичний аспект. *Економічний Вісник НТУУ «КПІ»*. 2017. С. 250 – 254. URL: https://doi.org/10.20535/2307-5651.14.2017.108778

40. Rietjens S. Hybrid CoE Strategic Analysis 22: A warning system for hybrid threats – is it possible? – Helsinki, Finland: Hybrid CoE, June, 2020. 10 p.

41. Кавун С. В., Пилипенко А. А., Ріпка Д. О. Економічна та інформаційна безпека підприємств у системі консолідованої інформації. Навчальний посібник. Вид. ХНЕУ. 2013. 364 с.

42. Якименко Ю. М., Мужанова Т. М., Легомінова С. В. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2020. № 4(12). С. 36-50.

43. Гришко С., Кодрул Р. Інформаційна безпека підприємства та організація системи управління інформаційною безпекою: матеріали Всеукраїнської науково-практичної конференції, м.Харків, 1 листопада 2022 р. Харків, 2022 (подано до друку)

44. Маркіна І. А., Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємництва. 2016. 3(1). 80 с.

45. Savolainen J. Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi): Hybrid CoE Working Paper. Helsinki, Finland: Hybrid CoE, 2019. 22 p.

46. Полозова Т. В. Формування інноваційно-інвестиційного механізму забезпечення конкурентоспроможності підприємства: монографія. Херсон: Видавничий дім «Гельветика», 2017. 592 с.

47. Соломіна Г.В. Забезпечення фінансово-економічної безпеки підприємництва: навчальний посібник. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. 234 с..

48. Limnéll J. Countering Hybrid Threats: Role of Private Sector Increasingly Important. Shared Responsibility Needed. Helsinki, Finland: Hybrid CoE, 2018. 8 p.

49. Kaikova, O., Terziyan, V., Tiihonen, T., Golovianko, M., Gryshko, S., Titova, L. Hybrid Threats against Industry 4.0 : Adversarial Training of Resilience. In R. Absi, & I. El Abbassi (Eds.), *EVF'2021 : 8th International Conference on Energy and City of the Future* (Article 03004). EDP Sciences. E3S Web of Conferences, 353.

50. Гришко С., Єфіміна О. Особливості захисту бізнесу в умовах гібридних загроз. *Матеріали І Міжнародної науково-практичної конференції «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта»* (Харків. 3 листоп. 2020) / За заг. ред. Т.В. Полозової. Харків: ХНУРЕ, 2020. С. 71-76.