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

ДОПУСТИТИ ДО ЗАХИСТУ
В ЕКЗАМЕНАЦІЙНІЙ КОМІСІЇ:

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства: практика та напрями вдосконалення»

Освітньо-професійна програма «Управління фінансово-економічною безпекою»
Спеціальність 073 «Менеджмент»
Рівень вищої освіти: другий (магістерський)

Здобувач **Іжболдін М.М.**

Науковий керівник,
д.держ.упр., професор_____ **Васільєва Л.М.**

науковий ступінь, посада

Дніпро – 2023

ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ АГРАРНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

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

З А Т В Е Р Д Ж У Ю
Зав. кафедри _____
«_____»_____ 202__р.

З А В Д А Н Н Я
на підготовку кваліфікаційної роботи

Іжболдіну Максиму Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: «Управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства: практика та напрями вдосконалення»

Науковий керівник: Васільєва Леся Миколаївна, д.держ.упр., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по ДДАЕУ від «09» жовтня 2023 року № 3051

2. Термін подання здобувачем роботи: 15.12.2023

3. Вихідні дані до роботи: навчально-методична література, нормативно-правові акти, пов'язані з темою роботи, річні звіти ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ».

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Теоретичні засади управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства 2. Практика управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства 3. Вдосконалення управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Наукова полеміка щодо дефініції «інформаційна безпека». Взаємозв'язок безпеки та інформаційної безпеки, який спрямований на збереження конфіденційності, цілісності та доступності інформації. Принципи інформаційної безпеки підприємства. Структура служби економіки та фінансів ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ». Загрози зовнішнього та внутрішнього оточення для ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ». Сильні сторони ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ». Організаційна структура щодо управління інформаційною безпекою на підприємстві. Загальний підхід до управління інформаційною безпекою. Основні складові методичного підходу до управління ризиками інформаційної безпеки.

6. Консультанти розділів роботи

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

7. Дата видачі завдання_____ _березень 2023 р._____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Проаналізувати фінансово-економічну характеристику підприємства та охарактеризувати роботу служби економічної безпеки підприємства та оцінка її стану за окремими складовими	Березень 2023	
2	Теоретичні засади управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства	Травень 2023	
3	Практика управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства	Липень 2023	
4	Вдосконалення управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства	Жовтень 2023	
5	Вступ. Висновки і пропозиції. Оформлення кваліфікаційної роботи	Грудень 2023	

Здобувач _____ _____Іжболдін М.М._____
(підпис) (прізвище та ініціали)

Науковий керівник _____ _____Васільєва Л.М._____
(підпис) (прізвище та ініціали)

ЗМІСТ

Р Е Ф Е Р А Т

Тема Управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства: практика та напрями вдосконалення

Кваліфікаційна робота: 72 ст. основного тексту, 4 табл., 19 рис., 7 додатків, 57 літературних джерел.

Об'єктом дослідження є процес управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства.

Предмет дослідження – теоретико-практичні підходи до удосконалення управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства.

Методи дослідження базуються на концепціях та працях вітчизняних науковців з питань використання інформаційних технологій. Методичні засади дослідження базуються на системному підході, який використовувався при дослідженні ефективності використання інформаційних технологій при забезпеченні економічної безпеки підприємств, методах індукції та дедукції, спостереження, систематизація та узагальнення, логічного аналізу та інші.

Узагальнено теоретичні засади управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства; проаналізовано фінансово-економічну характеристику підприємства; оцінено службу економічної безпеки підприємства та охарактеризувати її стан за елементами; розглянуто процес управління інформаційною безпекою в ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ»; запропоновано методичний підхід до управління ризиками інформаційної безпеки; надано рекомендації щодо застосування економіко-математичних методів та моделей в управлінні інформаційною безпекою для забезпечення економічної безпеки підприємства.

Результати використані ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» м.Павлоград Дніпропетровської області.

КЛЮЧОВІ СЛОВА

інформація, інформаційна безпека, державна інформаційна політика, загрози інформаційній безпеці, механізми, підприємницька діяльність

ANNOTATION

The topic of information security management in the context of ensuring the economic security of the enterprise: practice and directions for improvement

Qualification work: 72 st. of the main text, 4 tables, 19 figures, 7 appendices, 57 literary sources.

The object of the study is the process of information security management in the context of ensuring the economic security of the enterprise.

The subject of the study is theoretical and practical approaches to improving information security management in the context of ensuring the economic security of the enterprise.

Research methods are based on the concepts and works of domestic scientists on the use of information technologies. The methodological principles of the research are based on the systematic approach that was used in the study of the effectiveness of the use of information technologies in ensuring the economic security of enterprises, methods of induction and deduction, observation, systematization and generalization, logical analysis, and others.

The theoretical principles of information security management in the context of ensuring the economic security of the enterprise are summarized; the financial and economic characteristics of the enterprise were analyzed; evaluated the enterprise's economic security service and characterized its condition by elements; the process of information security management in PJSC «DTEK PAVOGRADVUHILLYA» was considered; a methodical approach to information security risk management is proposed; recommendations on the application of economic and mathematical methods and models in the management of information security to ensure the economic security of the enterprise are provided.

The results were used by PJSC «DTEK PAVOGRADVUHILLYA» in Pavlograd, Dnipropetrovsk region.

KEYWORDS

information, information security, state information policy, threats to information security, mechanisms, entrepreneurial activity

ВСТУП

Актуальність теми дослідження. Інформація настільки проникла на підприємства та в повсякденне життя, що стала майже необхідною. Це зрозуміло, оскільки інформація стала основою бізнес-операцій будь-якого підприємства. Кожен день у бухгалтерських і фінансових операціях є потенціал для помилок даних, пов'язаних з комп'ютером, неправильною сформованою інформацією, порушень внутрішнього контролю, крадіжок тощо. Через свою величезну цінність інформація та пов'язані з нею ресурси мають бути належним чином захищені. Цей захист інформації зазвичай називають інформаційною безпекою. Ризики інформаційної безпеки є стратегічним питанням, яким повинні ретельно займатися всі підприємства, як державні, так і приватні.

Підсумовуючи сказане, зазначимо, що актуальним є дане дослідження щодо практики та визначення напрямів удосконалення управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства.

Дану проблематику піднімали в своїх дослідженнях такі вчені: Аніловська Г.Я., Акімова Н.С., Васильців В.Г., Гончаренко Є.О., Дейнега О.В., Кирильєва Л.О., Мазник Л.В., Наумова Т.А., Яровенко Г.М. та ін. Проте, в науковій літературі залишається дискусійні питання щодо аналітичних загроз, додаткові елементи інформаційної безпеки в контексті забезпечення економічної безпеки підприємства, що і зумовило вибір теми дослідження.

Мета і завдання дослідження. Метою дослідження є визначення теоретико-методичних та практичних підходів щодо удосконалення управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства.

Досягнення поставленої мети вимагало вирішення наступних завдань:

– узагальнити теоретичні засади управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства;

– проаналізувати фінансово-економічну характеристику підприємства;

– оцінити службу економічної безпеки підприємства та охарактеризувати її стан за елементами;

– розглянути процес управління інформаційною безпекою в ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ»;

– запропонувати методичний підхід до управління ризиками інформаційної безпеки;

– надати рекомендації щодо застосування економіко-математичних методів та моделей в управлінні інформаційною безпекою для забезпечення економічної безпеки підприємства.

Об'єктом дослідження є процес управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства.

Предмет дослідження – теоретико-практичні підходи до удосконалення управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства.

Методи дослідження базуються на концепціях та працях вітчизняних науковців з питань використання інформаційних технологій. Методичні засади дослідження базуються на системному підході, який використовувався при дослідженні ефективності використання інформаційних технологій при забезпеченні економічної безпеки підприємств, методах індукції та дедукції, спостереження, систематизація та узагальнення, логічного аналізу та інші.

Інформаційною базою кваліфікаційної роботи стали вітчизняні та зарубіжні літературні джерела, матеріали інтернет-ресурсів, дані річної звітності досліджуваного підприємства.

Наукова новизна одержаних результатів присвячена удосконаленню управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства, а саме:

удосконалено:

- основні складові методичного підходу до управління ризиками інформаційної безпеки: ідентифікація активів, визначення загроз, оцінка вразливостей, оцінка ризиків, моніторинг, аналіз та аудит ризиків, визначення стратегій керування ризиками, вибір та впровадження контрольних заходів. Відповідно до визначеного методичного підходу до управління ризиками інформаційної безпеки запропоновано алгоритм взаємодії елементів процесу щодо управління ризиками інформаційної безпеки;

набуло подальшого розвитку:

- сформовано загальний підхід до управління інформаційною безпекою, який складається із базису (серцевини) і ряду глибинних розрізів, зокрема: директиви, контроль, аспект управління ризиками, організаційний вимір, вимір обізнаності;

- необхідність застосування економіко-математичних моделей, що дозволяє підприємствам більш раціонально розуміти витрати та ефективність заходів з інформаційної безпеки, сприяючи вирішенню важливих завдань у контексті економічної безпеки.

Апробація одержаних результатів. Основні теоретичні положення і практичні результати дослідження доповідались та обговорювались на всеукраїнській науково-практичній інтернет-конференції: «Молодь, наука, бізнес традиційні й нові аспекти досліджень» (м. Дніпро, 2023 р.), «Облік, аудит, оподаткування та звітність у системі забезпечення економічної стійкості підприємств» (м. Дніпро, 2023 р.).

Публікації. За результатами дослідження опубліковано 1 статтю, загальним обсягом 0,5 ум. друк. арк.

Дипломна робота складається з вступу, трьох розділів, висновків та пропозицій, додатків, списку використаних джерел 57 найменувань, містить 4 таблиці, 19 рисунків, 7 додатків. Основний зміст дипломної роботи викладено на 72 сторінках друкованого тексту.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1. Система забезпечення економічної безпеки підприємства: поняття та основні чинники, що формують відповідний її рівень

Забезпечення економічної безпеки підприємства є важливою умовою для його стабільності та успішності. Це необхідно здійснювати з ряду причин.

По-перше, забезпечення економічної безпеки захищає компанії від низки ризиків, включаючи економічні кризи, коливання валютних курсів, законодавчі зміни, стихійні лиха та інші негативні впливи.

По-друге, економічно стійкі підприємства уникають фінансових скандалів, банкрутства та інших проблем, які можуть зашкодити їхній репутації серед споживачів, інвесторів та партнерів.

По-третє, економічна безпека дозволяє підприємству інвестувати в нові проєкти та дослідження й розвиток. Це допомагає посилити їхню конкурентоспроможність та здатність конкурувати на ринку.

По-четверте, бізнес має бути економічно стійким, щоб витримувати конкуренцію на ринку, реагувати на зміни попиту та швидко адаптуватися до нових тенденцій.

По-п’яте, економічно стабільні підприємства можуть забезпечувати стійкі робочі місця, відраховувати податки та сприяти соціальному розвитку свого регіону.

Отже, забезпечення економічної стійкості компанії є важливим елементом її діяльності, який дозволяє їй підтримувати стабільність, зростання та довіру стейкхолдерів.

Що ж таке економічна безпека? Пропонуємо розглянути дану

категорія, як її інтерпретують науковці.

Економічна безпека - це стан стійкості та захищеності економічної системи від зовнішніх та внутрішніх загроз, що можуть спричинити негативні наслідки для її функціонування, стабільності та розвитку. Економічна безпека визначається рівнем захищеності економічних інтересів країни, підприємства чи окремої особи від різних загроз.

Баланюк І.Ф., Максимюк М.М. зазначають, що «економічна безпека це такий стан соціально-економічної системи держави, що стійко розвивається, яка дозволяє гарантовано забезпечувати захист національно-державних інтересів перед зовнішніх і внутрішніх загроз втрати стійкості розвитку» [4].

Гапак Н.М., Дочинець І.В. визначають економічну безпеку як «поєднання економічних, політичних та правових умов, яке забезпечує у довгостроковій перспективі виробництво максимальної кількості економічних ресурсів на душу населення ефективним способом» [13].

На думку Маркіної І.А., Дячкова Д. В. економічна безпека це «стан правових, виробничих та організаційних відносин, матеріально-інтелектуальних ресурсів, забезпечення стабільності діяльності, фінансової та комерційної успішності, науково-технічного та соціального розвитку» [31].

Ситник Г.В., Блакита Г.В., Гуляєва Н.М. вважають, що економічна безпека це «забезпечення статусу важливих видів діяльності підприємства, які реалізують його основні інтереси, захищеності від внутрішніх і зовнішніх загроз та дестабілізуючих факторів» [43].

Ярославський А.О., Правдюк Н. Л. визначають економічну безпеку як «кількісні та якісні характеристики підприємства, що відображають його здатність виживати та розвиватися в умовах зовнішніх та внутрішніх економічних загроз» [55].

На думку Смачило Т. В., Кахній М. І. економічна безпека «захист життєво важливих інтересів підприємства від внутрішніх і зовнішніх загроз шляхом реалізації економіко-правових, організаційних, інженерно-технічних

та соціально-психологічних заходів» [44].

Підсумовуючи вищенаведене можна узагальнити підходи до поняття економічна безпека (рис. 1.1).

Рис. 1.1. Узагальнення підходів до визначення сутності поняття «економічна безпека підприємства»*

**Сформовано автором*

Загалом, економічна безпека є важливою складовою сталого розвитку компанії, що сприяє її довгостроковому успіху та впливає на багато різних сфер бізнесу, від фінансів до репутації та інновацій.

Таким чином, економічна безпека підприємства - це можливість підприємства ефективно працювати в умовах фінансово-економічної нестабільності та своєчасно реагувати на зміни зовнішнього середовища. Цей процес передбачає також забезпечення захисту від внутрішніх і зовнішніх

загроз.

Економічна стійкість підприємства характеризується якісними та кількісними показниками серед яких можемо виділити рівень економічної безпеки підприємства як аналіз стану застосування підприємством ресурсів відповідно до критеріїв рівня його економічної безпеки. Для досягнення найвищого рівня економічної безпеки підприємство повинно забезпечити максимальну безпеку основних функціональних складових господарської діяльності. Рівень економічної безпеки підприємства залежить від низки факторів. Нижче наведені деякі з основних факторів, що впливають на економічну безпеку підприємства (рис. 1.2).

Рис. 1.2. Основні фактор, що впливають на економічну безпеку*

**Сформовано автором за джерелами* [28, 36, 46]

На думку Ільницька У. «існують й інші фактори економічної безпеки, які безпосередньо не пов'язані з виробництвом, але мають на нього вплив - поведінка, мораль, духовність людей» [22]. Кургузенкова Л.А. зазначає, що «базовим елементом забезпечення економічної безпеки підприємства може бути стратегічне планування і прогнозування діяльності підприємства» [26].

Економічна безпека підприємств в деякій мірі має залежність від економічної безпеки держави. Взаємозв'язок та взаємозалежність між цими двома елементами є важливим і може бути продемонстрований різними способами. «Економічна безпека залежить від економічної безпеки держави, регіону, оскільки в її основі лежить фінансовий та виробничий потенціал, а також перспективи розвитку підприємства» [17].

Можемо відмітити, що економічній безпеці підприємств притаманна подвійна природа. З однієї сторони, вона гарантує перспективу власного існування, з іншої сторони - являється складовою економічної безпеки вищої системи, що передбачає гарантію щодо здійснення певного функціоналу чи державою чи регіоном.

Отже, фактори, що формують належний рівень економічної безпеки підприємств різноманітні та є специфічними для кожної галузі. Проте існують і типові фактори, що мають спільні риси, що впливають на рівень економічної безпеки підприємств. Збалансоване та ефективне управління цими елементами може створити стійкий економічний фундамент для підприємств.

Система, спрямована на забезпечення економічної безпеки підприємства, є комплексною, враховує багато різних аспектів діяльності та дозволяє підприємству набути стабільності та конкурентоспроможності у мінливому економічному середовищі.

Таким чином, систему забезпечення економічної безпеки підприємства можна визначити як комплекс заходів та сукупність стратегій, які спрямовані на мінімізацію ризиків і забезпечення фінансового стану підприємства та стійкості його господарської діяльності.

1.2. Інформаційна безпека як складова економічної безпеки: сутність, зміст та принципи її забезпечення

В умовах сьогодення за наявності мінливого зовнішнього середовища, сучасного ведення бізнесу інформація та її захист є важливою складовою також і системи забезпечення економічної безпеки підприємства. Зростання процесу комп'ютеризації суспільства, що спостерігається протягом останніх десятиліть спричинило появу нових викликів щодо забезпечення інформаційної безпеки. Здійснимо порівняльний аналіз поняття «інформаційна безпека» яка трактується дослідниками цього питання (рис. 1.3).

Рис. 1.3. Наукова полеміка щодо дефініції «інформаційна безпека»

На нашу думку, інформаційну безпеку ми можемо визначити як таку ситуацію щодо захисту інформації від небажаного доступу, розголошення, видозміни, втрати тощо. Наголосимо, що у загальному формулюванні інформаційна безпека передбачає гарантування конфіденційності, цілісності та доступності інформації, яка використовується підприємством. Конфіденційність - забезпечення та збереження конфіденційної інформації від несанкціонованого доступу. Цілісність - забезпечення точності та повноти інформації шляхом запобігання несанкціонованої модифікації або знищення даних. Доступність - забезпечення доступу до інформації у необхідному обсязі та у відповідному часі (рис. 1.4). Ці три властивості інформації мають бути збережені в усіх станах інформації [4].

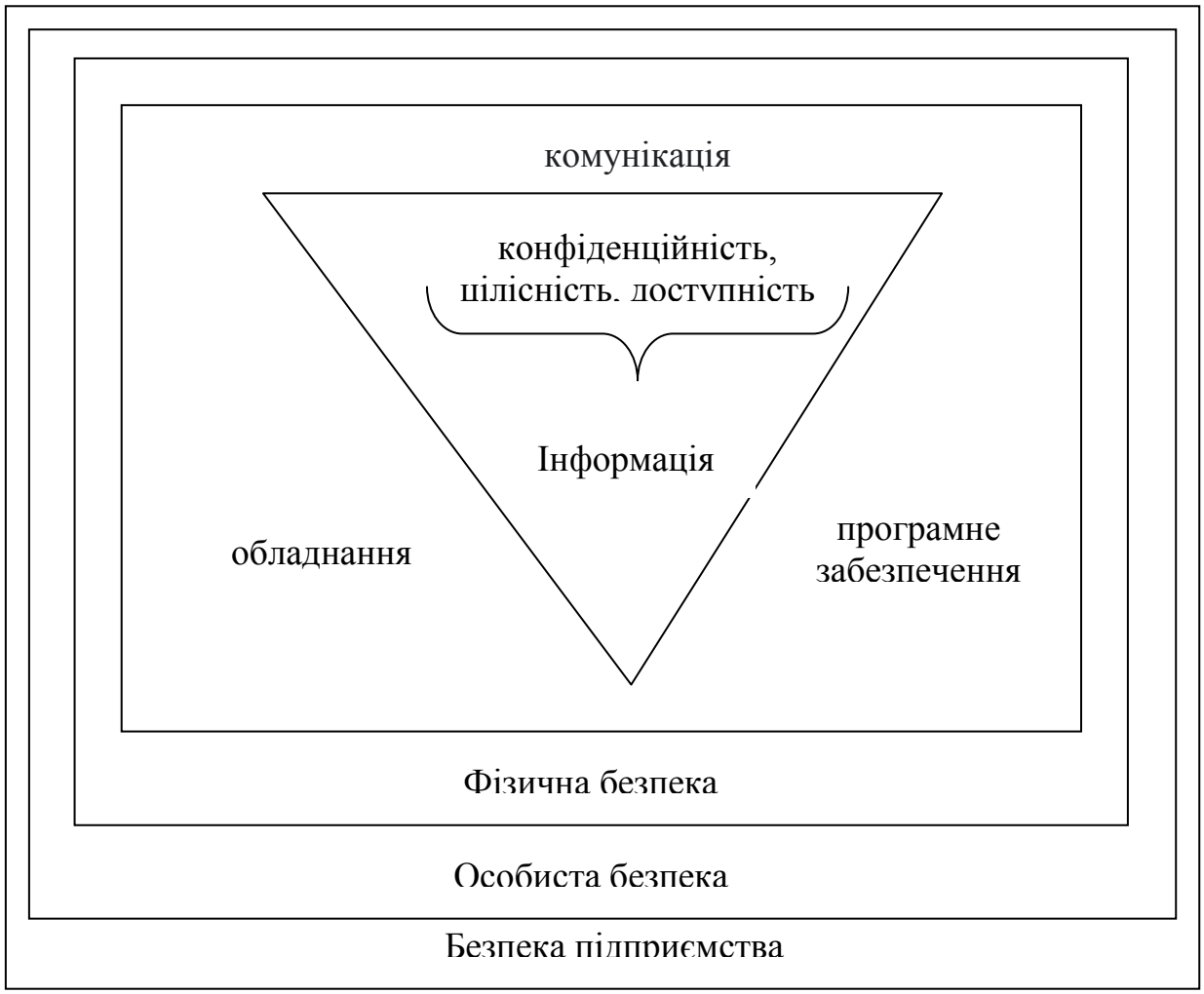


Рис. 1.4. Взаємозв’язок безпеки та інформаційної безпеки, який спрямований на збереження конфіденційності, цілісності та доступності інформації

На наше переконання це основоположна тріада щодо формування принципів інформаційної безпеки, вона являється запорукою надійного захисту інформації на підприємстві.

Існує багато факторів, які слід враховувати під час захисту інформації та пов'язаних з нею ресурсів, формально це процес інформаційної безпеки [50]. По-перше, це важливо для захисту інформації в усіх її різних станах. Ця теза вказує на те, що інформація повинна бути захищена - поки вона зберігається, поки вона обробляється або використовується, а також поки вона передається. Цей принцип інформаційної безпеки діє до інформації всіх типів, яка включає електронну або цифрову інформацію та друковані засоби масової інформації.

Крім того, інформаційна безпека спрямована на збереження конфіденційності, цілісності та доступності інформації. Ці три властивості, які ми навели вище, або характеристики інформації мають бути збереженими в усіх згаданих раніше інформаційних станах. Конфіденційність інформації можна визначити як властивість, яка гарантує, що інформація не стане доступною та не розкрита несанкціонованим особам, організаціями або процесами. Цілісність, вказує на те, що це власність, яка спрямована на забезпечення та захист точності та повноти інформаційних активів. Нарешті, доступність - це властивість інформації бути доступною та придатною для використання на вимогу уповноваженої особи, підприємства або процесу.

Зважаючи на це, можна стверджувати, що коли інформація захищена належним чином, ці принципи (конфіденційність, цілісність та доступність) значною мірою гарантують, що інформація та пов'язані з нею ресурси підприємства убезпечені від втрати, викрадення або використання не за призначенням. Хоча ці три властивості інформації, перш за все становлять інформаційну безпеку, інші властивості також можуть бути задіяні, такі як: автентичність, підзвітність, неспростовність і надійність. Крім того, при реалізації інформаційної безпеки, загрози та вразливість інформації і пов'язані ресурси, а також вплив виявлених загроз, можуть бути пом'якшені.

Проаналізувавши наукову літературу в якій характеризуються підходи науковців щодо характеристики принципів інформаційної безпеки підприємства можемо зробити узагальнений підхід до формування принципів інформаційної безпеки підприємства (табл. 1.1).

Таблиця 1.1

Принципи інформаційної безпеки підприємства*

Принцип	Характеристика
Конфіденційність	Забезпечте конфіденційність інформації, обмеживши доступ до неї лише тим, хто має до неї авторизований доступ
Цілісність	Забезпечте цілісність інформації, захищаючи її від несанкціонованих змін і випадкового пошкодження
Доступність	Переконайтеся, що інформація надається лише тим, хто має право доступу до неї
Автентичність	Переконайтеся в достовірності інформації, підтвердивши її джерело та не змінюючи під час передачі
Надійність	Забезпечення надійності інформації, захищаючи її від випадкової та навмисної втрати та знищення
Універсальність	Переконайтеся, що заходи безпеки інформації впроваджуються відповідно до всіх вимог і стандартів, застосовних до такої діяльності
Комплексність	Забезпечте захист інформації на всіх етапах, від збору та зберігання до передачі та обробки
Випереджувальність	Виявляйте та запобігайте потенційним загрозам інформаційній безпеці до впровадження

**Узагальнено автором на основі джерел* [1, 7, 15]

Управління інформаційною безпекою, як і будь-який інший процес управління, зазвичай має здійснюватися за підходом зверху вниз. Це підтверджується Кузьомко В. [25], оскільки він стверджують, що інформаційна безпека є відповідальністю корпоративного управління, яка

лежить на найвищому керівництві підприємства. Таким чином, управління інформаційною безпекою має здійснюватися з чітким баченням і цілями, які вона прагне задовольнити вимоги вищого керівництва.

Ці цілі слід визначати, беручи до уваги, що процес управління інформаційною безпекою є складним і багатовимірним процесом. Кожен із багатьох аспектів інформаційної безпеки слід ретельно розглядати під час впровадження управління інформаційною безпекою, щоб уникнути впровадження одностороннього процесу управління, яка врешті-решт зазнає невдачі.

Кузьомко В. [25] також стверджує, що точна кількість вимірів і їх точний зміст не є найважливішим питанням, а скоріше розуміння того, що інформаційна безпека насправді є багатовимірною дисципліною і що різні виміри колективно сприяти захисту інформації та пов’язаних ресурсів.

«Метою інформаційного забезпечення є своєчасне надання необхідної і достатньої інформації для прийняття управлінських рішень, що забезпечують ефективну діяльність підприємства» [15].

На думку Г.Я. Аніловської, «одним із методів забезпечення інформаційної безпеки підприємства є стандартизація, елементами якої виступають форми існування і подання інформації у цілому, а зв’язками – операції перетворення інформації» [2].

Наголосимо, що не існує універсального рішення для захисту інформації. Згодом це означає, що кожне підприємство має впроваджувати спеціально адаптований підхід до інформаційної безпеки, унікальний для потреб підприємства, спрямований на ризики для його інформації та пов’язаних ресурсів. Таким чином, певна форма оцінки ризику повинна допомогти визначити ризики, які необхідно розглянути, що, у свою чергу, забезпечить оптимальний захист інформаційних ресурсів підприємства. Ризики для інформаційної безпеки розглянемо у наступному підрозділі даного дослідження.

1.3. Ризики в системі інформаційної безпеки підприємства

Загроза є потенційною причиною небажаного інциденту, який може завдати шкоди системі або підприємству. Вразливість - це слабкість інформаційного ресурсу або контролю, яка може бути використана однією або кількома загрозами. Нарешті, випадки, коли ці вразливості використовуються загрозами, можуть бути небезпечними наслідками для підприємства. Таким чином, впливу подібних ситуацій теж має бути приділено значну увагу під час вирішення питань інформаційної безпеки. Такі фактори вразливості, загрози та вплив на інформаційну безпеку, по суті, становлять ризик інформаційній безпеці. Ці ризики повинні розглядатися комплексно, щоб захистити інформацію.

Індустрія інформаційної безпеки, так звана «Infosec», передбачає певну рівновагу конкурентних факторів і тому її можна співвіднести з управлінням ризиками. Метою є максимізація позитивних результатів і мінімізація негативних наслідків. Підприємства в своїй діяльності приміняють принципи управління для визначення рівня ризику при впровадженні системи.

Визначення ризику залежить від різних видів бізнесу та середовища. У контексті інформаційної безпеки ризик визначається як комбінація ймовірності події та її наслідків [5]. Васильців В.Г. визначає ризик як ймовірність того, що агент загрози буде використовувати вразливість системи, щоб створити втрату конфіденційності, цілісності та наявність активу. Загроза – це потенційна причина інциденту, який може призвести до шкоди системі чи підприємству [9].

Зеленко О.О., загроза також визначається як будь-яка особа або об’єкт, що становить небезпеку для активу [18]. Вразливість визначається як слабкість активу або групи активів, які можуть бути використані однією або декількома загрозами [23]. Легомінова С.В. визначає вразливість як слабкість, недолік, діра або будь-що, чим може скористатися загроза, яка потім призводить до згубного результату [27].

Виходячи з наведених вище визначень, можна зробити висновок, що ризики для інформаційної безпеки можуть бути результатом процесів модифікації, руйнування, виготовлення, розголошення, переривання, відмова в обслуговуванні та крадіжка обладнання, програмного забезпечення або даних. Для ефективного управління цими ризиками кожне підприємство має керуватися регулярними та ефективними заходами з управління ризиками для розуміння природи цих ризиків та можливі наслідки.

Важливість управління ризиками інформаційної безпеки продовжує зростати в усьому світі в результаті збільшення кількості порушень, які впливають на захист інформаційних ресурсів, а отже, і господарської діяльності підприємства.

Відсутність належним чином реалізованих заходів безпеки для пом’якшення зростання ризиків інформаційної безпеки було відображено в рекомендаціях та вимогах урядів країн з розвиненою економікою щодо ведення регулярних і ефективних програм управління ризиками. Наприклад, закон Сарбейнса-Окслі 2002 р., який є обов’язковим для всіх підприємств, що працюють в США, незалежно від їх розміру чи бізнесу, вимагають, щоб емітенти цінних паперів, які публічно продаються на фінансових ринках США використовували і анонсували модель управління ризиками для своїх зацікавлених сторін [56]. Крім того, один із основних обов’язків агентств відповідно до FISMA (Федеральний закон про модернізацію інформаційної безпеки) США має проводити регулярну оцінку ризиків [56].

Ризик інформаційної безпеки розглядає потенційний інцидент однієї або кількох загроз, які використовують вразливість інформаційного ресурсу, ймовірність виникнення таких інцидентів і вплив, який вони можуть мати, коли вони справді трапляються. У більшості випадків у сфері інформаційної безпеки фізичні, технічні та операційні проблеми, які проявляються на підприємстві, вирішуються шляхом запровадження засобів контролю, щоб пом’якшити відповідні ризики. Ця реалізація засобів контролю для зменшення ризиків інформаційної безпеки зазвичай називається обробкою

ризиків.

Однак, перш ніж підприємство зможе почати розглядати будь-які ризики, пов’язані з інформацією, середовище ризиків інформаційної безпеки підприємства має бути належним чином оцінено [53]. Діяльність з оцінки ризиків інформаційної безпеки загалом складається з трьох частин (рис. 1.5).

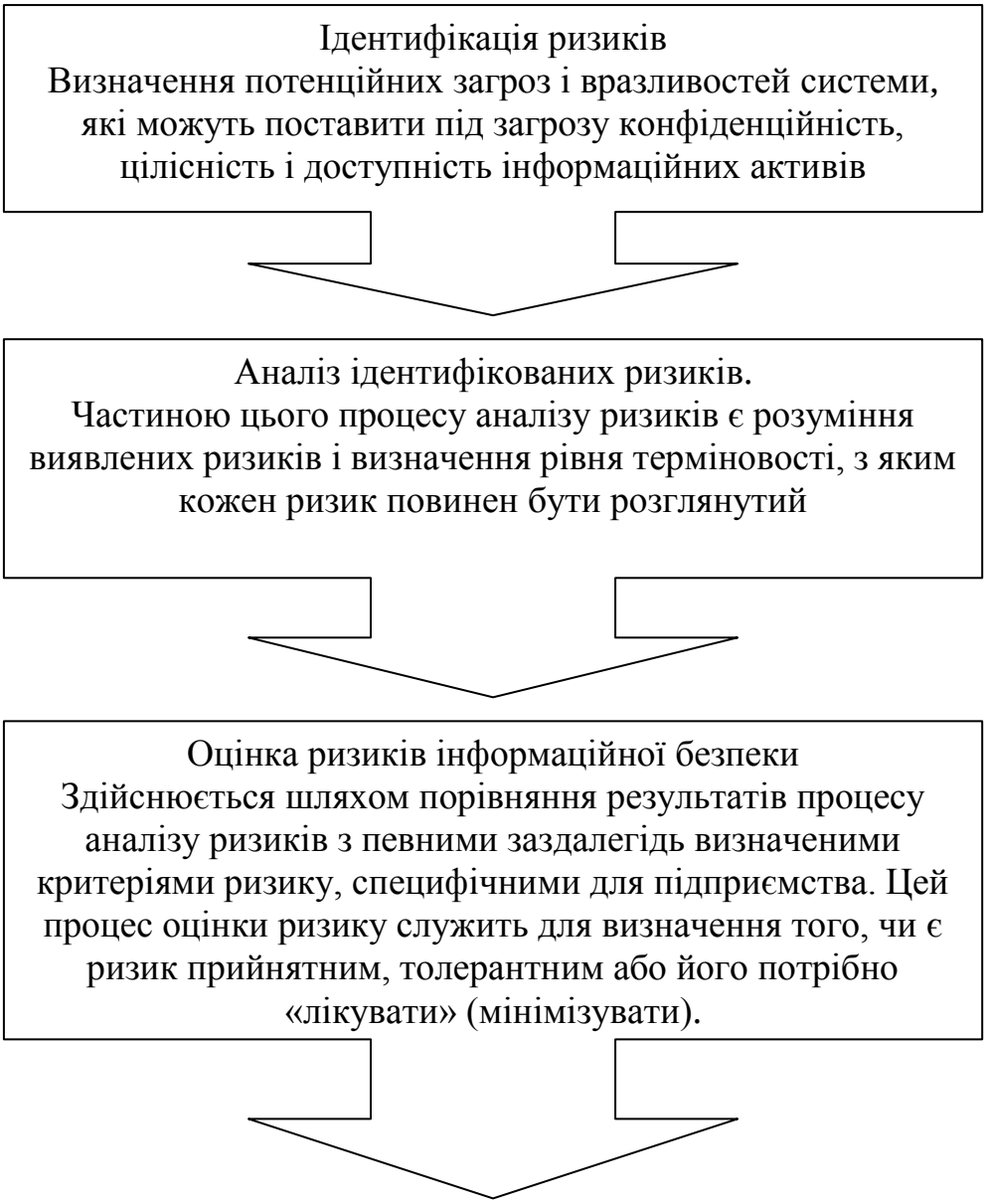


Рис. 1.5. Кроки щодо оцінки ризиків інформаційної безпеки

Наголосимо, ці три процеси ідентифікації, аналізу та оцінки ризиків інформаційної безпеки спільно сприяють оцінці інформаційних ризиків. Цю діяльність з оцінки ризиків потрібно постійно повторювати, щоб усунути

нові загрози та вразливі місця, а також задовольнити ризики, які є результатом змін у середовищі, системах та інфраструктурі. Однак оцінка ризику інформаційної безпеки лише класифікує ідентифіковані ризики відповідно до їх потенціалу завдати шкоди підприємству в разі реалізації. Ці ризики після їх оцінки все ще потребують пом'якшення до прийнятного рівня.

Формальна діяльність з обробки ризиків служить для пом'якшення ризиків інформаційної безпеки після завершення задовільного оцінювання. У рамках цієї діяльності ризики інформаційної безпеки можна розглядати багатьма способами [51]:

- модифікація ризику - включає введення, видалення або зміну засобів контролю, щоб залишковий ризик був на прийнятному рівні після повторної оцінки;

- утримання ризику - рішення навмисно зберегти ризик, не вживаючи жодних подальших дій для зменшення ризику;

- уникнення ризику - коли вживаються дії для уникнення діяльності або стану, що створює ризик;

- розподіл ризиків - коли ризик розподіляється з іншими сторонами найбільш ефективним способом.

Результат «лікування» ризику інформаційної безпеки слід оцінити після завершення, щоб визначити, чи вдалось «лікування», зменшило або змінило певний ризик до прийнятного рівня. Як згадувалося раніше, засоби контролю інформаційної безпеки впроваджуються для «лікування» цих ризиків і пом'якшення їх до прийнятного рівня. Проте засоби контролю інформаційної безпеки повинні бути належним чином доведені до відома всіх внутрішніх або зовнішніх користувачів інформації підприємства.

Цілі інформаційної безпеки повинні узгоджуватися з корпоративними цілями підприємства, щоб гарантувати, що інформація найкращим чином підтримує операційні процеси всередині підприємства. На додаток до чітких цілей щодо інформаційної безпеки, згаданих раніше, управління

інформаційною безпекою та пов’язані з нею ризики потребує абсолютної відданості вищого керівництва, щоб воно було успішним [47]. Це критично важливе зобов’язання та цілі вищого керівництва щодо інформаційної безпеки зазвичай мають передаватися через корпоративну політику інформаційної безпеки, яка є основою будь-якої успішної спроби управління інформаційною безпекою [35]. Ця корпоративна політика інформаційної безпеки забезпечує бачення інформаційної безпеки всередині підприємства та є стратегічною за своєю природою. Таким чином, така корпоративна політика інформаційної безпеки має бути концептуальною, достатньо загальною та статичною, замість того, щоб містити багато деталей про поточний бізнес-ландшафт або містити деталі про технічні проблеми. Незважаючи на те, що ця політика здебільшого має залишатися досить статичною, її слід, однак, регулярно переглядати та коригувати, коли необхідно, щоб забезпечити її актуальність. Однак через відсутність технічних деталей, передбачених цією політикою, її слід доповнити достатніми вторинними політиками та процедурами, які забезпечують необхідну підтримку в цьому.

Другий рівень політик інформаційної безпеки також називають вторинними, пов’язаний з проблемою або допоміжними політиками, і зазвичай вони більш детальні, специфічні та динамічні, ніж політика корпоративної інформаційної безпеки високого рівня. Ці допоміжні політики також враховують як поточний технологічний або бізнес-ландшафт, так і поточні та майбутні проєкти всередині підприємства [24]. Крім того, ці допоміжні політики інформаційної безпеки часто присвячені розгляду однієї теми, такої як використання Інтернету або електронної пошти, класифікація інформації, контроль доступу або безпека мережі, і тому їх часто називають проблемними [19]. Розглядаючи ці різноманітні теми, допоміжні політики інформаційної безпеки спрямовані на вирішення технічних, фізичних та операційних проблем інформаційної безпеки на підприємстві. Згодом, запроваджуючи ці політики, підприємство ставить собі за мету розглядати

унікальні та специфічні ризики, пов’язані з його інформаційними ресурсами, щоб пом’якшити ризики до прийнятного рівня.

Проте простого визначення та донесення до користувачів інформації цілей і бачення підприємства щодо інформаційної безпеки, від стратегічної корпоративної політики до операційних і технологічних питань допоміжної політики, недостатньо для того, щоб гарантувати, що бажана поведінка інформаційної безпеки буде виконуватися. Таким чином, користувачам корпоративної інформації необхідно постійно нагадувати та навчати різним підходам щодо побудови політики інформаційної безпеки, щоб мати найбільш ефективний вплив на поведінку людей у питаннях інформаційної безпеки або диктувати їх.

Висновки до першого розділу

1. Економічна безпека підприємства - це можливість підприємства ефективно працювати в умовах фінансово-економічної нестабільності та своєчасно реагувати на зміни зовнішнього середовища. Цей процес передбачає також забезпечення захисту від внутрішніх і зовнішніх загроз. Забезпечення економічної стійкості компанії є важливим елементом її діяльності, який дозволяє їй підтримувати стабільність, зростання та довіру стейкхолдерів.

2. Зазначено, що інформаційну безпеку можна визначити як такий стан щодо захисту інформації від небажаного доступу, розголошення, видозміни, пошкодження або знищення тощо. Наголосимо, що у загальному формулюванні інформаційна безпека передбачає гарантування конфіденційності, цілісності та доступності інформації, яка використовується підприємством.

3. Виділено взаємозв’язок безпеки та інформаційної безпеки, який спрямований на збереження конфіденційності, цілісності та доступності інформації. На наше переконання це основоположна тріада щодо формування

принципів інформаційної безпеки, яка являється запорукою надійного захисту інформації на підприємстві.

4. Індустрія інформаційної безпеки, так звана «Infosec», передбачає певну рівновагу конкурентних факторів і тому її можна співвіднести з управлінням ризиками. Ризики для інформаційної безпеки можуть бути результатом процесів модифікації, руйнування, виготовлення, розголошення, переривання, відмова в обслуговуванні та крадіжка обладнання, програмного забезпечення або даних. Для ефективного управління цими ризиками кожне підприємство має керуватися регулярними та ефективними заходами з управління ризиками, для розуміння природи цих ризиків та можливих наслідків.

5. Встановлено, що перш ніж підприємство зможе почати розглядати будь-які ризики, пов’язані з інформацією, середовище ризиків інформаційної безпеки підприємства має бути належним чином оцінено. Діяльність з оцінки ризиків інформаційної безпеки загалом складається з трьох процесів: ідентифікація ризиків; аналіз ідентифікованих ризиків; оцінка ризиків інформаційної безпеки.

6. Наголошено, що формальна діяльність з обробки ризиків служить для пом’якшення ризиків інформаційної безпеки після завершення задовільного оцінювання. У рамках цієї діяльності ризики інформаційної безпеки можна розглядати багатьма способами: модифікація ризику, включає введення, видалення або зміну засобів контролю, щоб залишковий ризик був на прийнятному рівні після повторної оцінки; утримання ризику, рішення навмисно зберегти ризик, не вживаючи жодних подальших дій для зменшення ризику; уникнення ризику, коли вживаються дії для уникнення діяльності або стану, що створює ризик; розподіл ризиків - коли ризик розподіляється з іншими сторонами найбільш ефективним способом.

РОЗДІЛ 2. ПРАКТИКА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1. Фінансово-економічна характеристика ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ»

Приватне акціонерне товариство «ДТЕК ПАВОГРАДВУГІЛЛЯ» було створене 02 квітня 1997 р., яке знаходиться за адресою 51400, Дніпропетровська обл., м.Павлоград, вул. Соборна, 76. Генеральний директор підприємства - Воронін Сергій Анатолійович. Розмір статутного капіталу складає 1395431 тис. грн.

Основний вид діяльності: 05.10 «добування кам'яного вугілля».

Інші: 01.11 «вирощування зернових культур (крім рису), бобових культур і насіння олійних культур»; 01.19 «вирощування інших однорічних і дворічних культур»; 85.32 «професійно-технічна освіта».

Через зменшення залишив кам’яного палива у наступному десятилітті Група ДТЕК має на меті розробляти проєкти в газовидобувній галузі, трейдингу і розподільних мережах. Організація планує запроваджувати підхід щодо «відкритих інновацій» та перейти з «постачальника енергії в постачальника рішень й інтегратора нових технологій».

Компанія є частиною вертикально інтегрованої енергетичної Групи ДТЕК і, відповідно, значна частина її продукції продається підприємствам, пов’язаним з ДТЕК. В результаті цього, Компанія проводить значні операції і має суттєві залишки за операціями з іншими компаніями Групи «ДТЕК», які є пов’язаними сторонами за ознакою спільного контролю.

Проаналізуємо майновий стан підприємства за аналізований період на підставі даних наведених в додатку А. Група провела переоцінку своїх основних засобів станом на 30 червня 2018 року. Переоцінка була проведена

на підставі звітів незалежних оцінювачів, які мають визнану кваліфікацію та професійний досвід оцінки майна, аналогічного оцінюваній власності за своїм розташуванням та категорією, а це в свою чергу призвело до збільшення вартості майна за досліджуваний період на 70,46 %. За станом на 31 грудня 2022 року товарно-матеріальні запаси показані за вирахуванням знецінення на застарілі ТМЗ в сумі 535362,0 гривень (на 31 грудня 2018 року відповідно 699261,0 тис. гривень).

Оцінка балансової вартості дебіторської заборгованості від пов'язаної компанії станом на 31 грудня 2022 року значна частка дебіторської заборгованості групи припадала на пов'язану особу під спільним контролем Групи DTEK Energy BV. Протягом 2022 року, Група нарахувала додатковий резерв під очікувані кредитні збитки у розмірі 3851095 тисяч гривень у зв'язку зі збільшенням кредитних ризиків щодо пов'язаної компанії, обумовлених, в першу чергу, військовим станом в Україні. Внаслідок цих подій, управлінський персонал Групи переглянув ставку очікуваних кредитних збитків з 8,41% (12-місячної), що використовувалась станом на 31 грудня 2021 року, до 31% (протягом періоду існування фінансового інструменту) станом на 31 грудня 2022. Також, упродовж 2022 року більша частина дебіторської заборгованості від пов'язаної компанії була реструктуризована. В результаті цієї події Групою у 2022 році було визнано витрати (дисконт) при модифікації фінансових активів у розмірі 4664559 тисяч гривень. Станом на балансову дату, дебіторська заборгованість від пов'язаної компанії була оцінена як кредитно-знецінена.

Що стосується власного капіталу підприємства, то за досліджуваний період його сума збільшилася майже в 2 рази і в 2022 р. становила 18124746,0 тис.грн. Станом на 31.12.2022 року резервний капітал становив 19 351 тис. грн., що становить 1,4 % від зареєстрованого капіталу компанії. Протягом року резервний капітал не зазнав змін. Станом на 31.12.2020р. резервний капітал враховується у складі нерозподіленого прибутку, та у окрему статтю (рядок 1415 «Резервний капітал») не виділявся. Як правило

резерв створюється під судові позови, подані проти Групи, сума резерву станом на 31 грудня 2021 року була використана до кінця 2022 року. Керівництво отримало належні юридичні консультації та вважає, що в результаті цих судових позовів не буде понесено значних збитків, що перевищували б вже нараховані суми.

Основні засоби являються основою виробничої діяльності будь-якого підприємства (додаток Б). В ПАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» основні засоби враховуються за переоціненою вартістю за вирахуванням накопиченого зносу і резерву на знецінення, якщо необхідно. У 2022 році витрати на амортизацію у сумі 9613313 тис. грн (у 2021 році - 9735645 тис. грн) були включені до складу собівартості реалізованої продукції, а 91274 тис. грн (у 2021 році - 62488 тис. грн) - до складу адміністративних витрат.

Показники функціонального стану основних засобів включають різноманітні технічні та експлуатаційні параметри, що визначають, наскільки ефективно основні засоби виконують свою функцію та в якому стані вони знаходяться. Станом на початок 2022 р. коефіцієнт зносу склав 42,29 %, що свідчить про те, що основний засіб залишився в експлуатації на 57,71% вартості його первісної вартості, а станом на кінець року цей показник становив 2,89%, що свідчить про те, що протягом року зменшується темп старіння або фізичного зносу основних засобів. Це вказує на те, що протягом року були проведені ремонтні роботи та заміна частини обладнання, що дозволяє зберігати актив у гарному стані та знижувати темпи його фізичного зносу. У цілому, це позитивний сигнал і може свідчити про ефективне управління та збереження активів підприємства.

Фінансова стійкість підприємства вказує на його здатність витримувати фінансові труднощі та зберігати стабільність у довгостроковій перспективі. Це важливий показник для оцінки фінансового здоров'я підприємства і впливає на його можливість розвиватися, виконувати свої функції та залишатися конкурентоспроможним. На рис. 2.1 та 2.2 наведено деякі показники фінансової стійкості ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» за

2018-2022 рр., а саме показники: структури капіталу та стану основного капіталу.

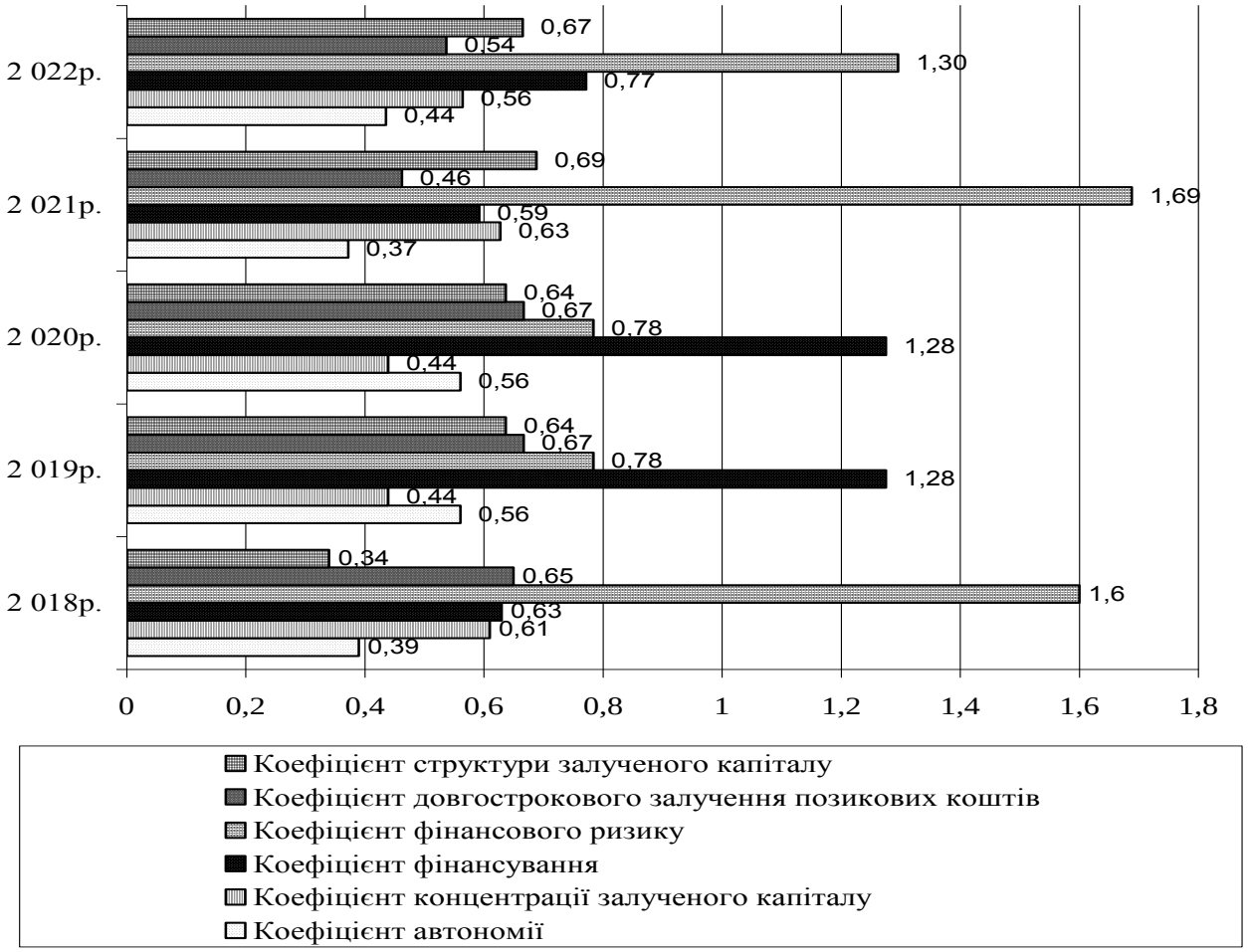


Рис. 2.1. Оцінка фінансової стійкості ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» в розрізі структури капіталу, 2018-2022 рр.

Для зниження ризику ліквідності здійснюється диверсифікація в розрізі контрагентів та оптимізація умов договорів у частині термінів оплати, реалізуються програми зі зниження операційних витрат. Так, за аналізований період коефіцієнт фінансового ризику знизився на 18, 75% не дивлячись на те, що країни перебуває в стані війни. Коефіцієнт фінансування мав тенденцію до збільшення за аналізований період відповідно на 22,22%, що свідчить про зміну структури фінансування підприємства це було частиною стратегічних рішень підприємства для досягнення конкретних цілей щодо оптимізації витрат.

Політика ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» стосовно управління

капіталом націлена на забезпечення і підтримку оптимальної структури капіталу для зменшення загальних витрат на капітал та гнучкості, необхідних для доступу компанії до ринків капіталу. Керівництво намагається зберігати баланс між більш високою доходністю, яку можна досягти при вищому рівні позикових коштів, та перевагами і стабільністю, які забезпечує стійка позиція капіталу. Протягом звітного періоду не було змін у підході до управління капіталом.

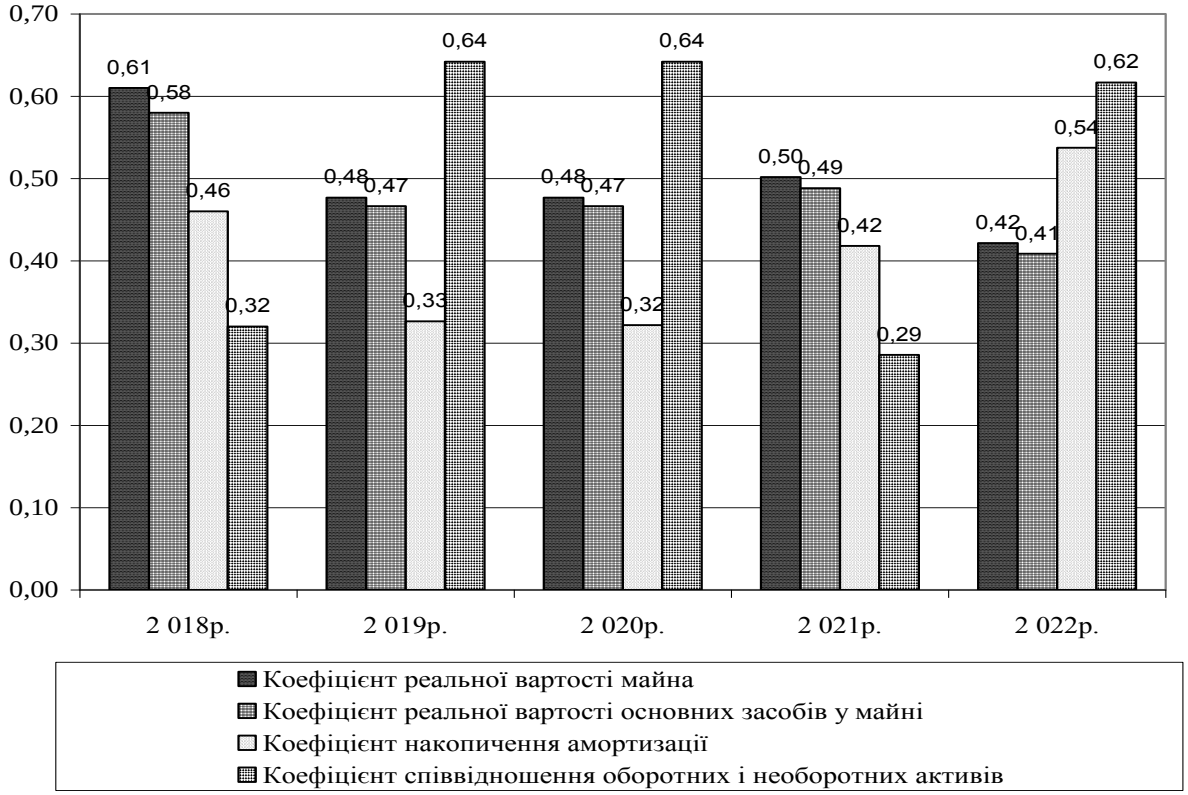


Рис. 2.2. Оцінка фінансової стійкості ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» в розрізі стану основного капіталу, 2018-2022 рр.

Коефіцієнт реальної вартості майна зменшився на 31,15% на що в свою чергу вплинуло зростання коефіцієнту накопичення амортизації відповідно на 17,39%. Коефіцієнт співвідношення оборотних і необоротних активів зріс майже в 2 рази і в 2022 р. становив 0,62 і свідчить про те, що , ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» має достатній рівень оборотної активності, що може бути важливим для швидкого вирішення фінансових зобов’язань, про збалансовану структуру активів, де якась частина активів призначена для

швидкого обороту, а інша - для довгострокового використання. Значення більше 0,5 вказує на те, що , ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» може підтримувати свої довгострокові зобов'язання, оскільки частина активів вкладена в необоротні активи.

Таким чином, можемо стверджувати, що якщо це необхідно, ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» матиме достатню ліквідність, щоб продовжувати обслуговувати операційні потреби, а також здійснювати платежі відповідно до ключових умов реструктуризації. Проте ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» не зможе здійснити погашення своїх запозичень згідно з початковим або прискореним графіком (до завершення реструктуризації).

Аналізуючи фінансові результати (додаток В) та показники ділової активності (додаток Д) відмітимо, що у 2022 році ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» продала 11,282 тисяч тонн вугілля та 119 тисяч МВТ-год покупної електроенергії на експорт (у 2021 році - 13,471 тисяч тонн вугілля та 2,704 тисяч МВТ-год покупної електроенергії на експорт). ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» визнає виручку від продажу вугілля в момент часу, а виручку від продажу електроенергії - з плином часу. Інша виручка є несуттєвою. За аналізований період виручка зросла на 32,02%, а прибуток зріс в 9,7 разів є значущим та є результатом ефективного управління витратами, покращенням операційної ефективності або інших стратегічних ініціатив.

Показники ділової активності вказують на різні аспекти ефективності та оборотності бізнесу. Зниження коефіцієнта обертання капіталу на 22,9% є результатом затримок у виробництві, недостатньої оборотності запасів, простою виробництва в свою чергу все це пов’язано зі значними втратами обладнання під час масованих ракетних ударів в 2022 р., що впливають на ефективність використання капіталу. При цьому коефіцієнт обертання власного капіталу в 2022 р. склав 1,51 і свідчить про те, що підприємство генерує прибуток, що перевищує його власний капітал в 1,51 рази. Це може

свідчити про ефективне використання власного капіталу.

На останок проведемо комплексну рейтингову оцінку). ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» (Додаток Е) інтегрований показник фінансового стану за досліджуваний період знаходиться в межах 8,46-8,65 і вказує на досить високий рівень фінансового стану відповідно рейтинг фінансового стану – А. Підхід Групи ДТЕК, до якої належить ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ», до ризик-менеджменту передбачає комплексну систему внутрішнього контролю та управління ризиками, засновану на стратегічному та поточному плануванні. У складі організаційної структури ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» функціонує Департамент з внутрішнього контролю та управління ризиками. Функція ризик-менеджменту представлена в ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» як на рівні корпоративного центру, так і на рівні підприємств.

У звітному періоді ризики, пов’язані із війною, мали значний вплив на підприємство. Але, незважаючи на всі перешкоди і завдяки своєчасним заходам з управління ризиками компанія, змогла забезпечити безперебійну діяльність.

2.2. Оцінка служби економічної безпеки підприємства та характеристика її стану за елементами

Ефективність реагування на загрози економічній безпеці значною мірою залежатиме від своєчасного реагування на наслідки подій, що впливають на рівень економічної безпеки та зрештою від витрат для бізнесу. невизначеність і змушені пристосовуватися до мінливого зовнішнього середовища. Це призводить до високих ризиків для діяльності. У зв’язку з цим особливого значення набуває забезпечення економічної безпеки ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ», що одним із головних завдань, яке стоїть перед керівництвом підприємства - створення ефективної системи управління економічною безпекою для вирішення питань щодо забезпечення

економічної безпеки в розрізі спектру актуальних викликів і загроз. Ефективність реагування на загрози економічній безпеці значною мірою залежить від оперативної реакції на результативність подій, які впливають на рівень економічної безпеки і в кінцевому підсумку на вартість підприємства.

Відмітимо, що на підприємстві немає спеціалізованого відділу економічної безпеки, всі обов'язки, пов'язані з забезпеченням економічної безпеки покладені на працівників служби економіки та фінансів. Чисельність служби складає 31 людина, згідно штатного розкладу не вистачає 6 осіб. Організаційна схема даної служби наведена на рис. 2.3.

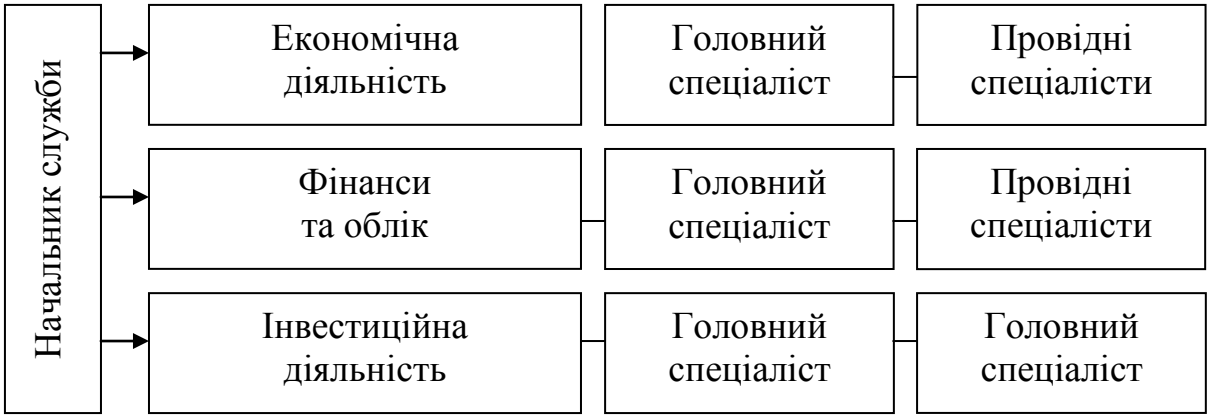


Рис. 2.3. Структура служби економіки та фінансів
ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ»

Забезпечення економічної безпеки ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» - це завдання, яке вимагає взаємодії між різними підрозділами та працівниками. Хоча економічний і фінансовий сектори відіграють важливу роль у цьому процесі, відповідальність за економічну безпеку розподілена між різними функціональними сферами та відділами. Розглянемо деякі аспекти роботи працівників служби економіки та фінансів:

- здійснюється розробка фінансових стратегій на різні часові проміжки;

- проводиться аналіз щодо ефективності використання фінансових результатів, витрат, надаються пропозиції щодо їхнього управління, з метою мінімізації ризиків;

- розробляються стратегії щодо оптимізації управління оборотним капіталом;

- проводиться фінансовий аналіз діяльності підприємства з метою прийняття управлінських стратегічних рішень;

- розробляються стратегії щодо мінімізації та ефективного управління ризиками;

- що стосується забезпечення інформаційної безпеки, то воно передбачає здійснення моніторингу стандартів безпеки даних та захист інформації від несанкціонованого доступу.

В ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» враховують те, що забезпечення економічної безпеки є сукупним завданням, а ключовим стержнем успіху в цій сфері є співпраця між різними функціональними секторами.

Для кращого розуміння стану економічної безпеки ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» проведемо оцінку факторів з точки зору зовнішнього та внутрішнього середовища (рис. 2.4):

- через зменшення залишив кам'яного палива у наступному десятилітті Група ДТЕК має на меті розробляти проєкти в газовидобувній галузі, трейдингу і розподільних мережах. Організація планує запроваджувати підхід щодо «відкритих інновацій» та перейти з «постачальника енергії в постачальника рішень й інтегратора нових технологій»;

- єдиним конкурентом ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» є ДП «Добропіллявугілля-видобуток», враховуючи те, що ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» належить до компанії ДТЕК, яка має закритий цикл «видобуток-збагачення-перетворювання-розподілювання» це дає змогу працювати більш ефективно;

- державні видобувні підприємства втрачають свою частку ринку через брак фінансування, що має дуже негативні наслідки для їхньої діяльності. Через низьку технологічну складову державних підприємств ДТЕК займає домінуючу позицію на енергетичному ринку країни та є монополістом, що

позитивно сказується на його економічній безпеці;

- через повномасштабне вторгнення ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» зазнає значних збитків через обстріли, через погіршення економічного, соціально-демографічного фактору.

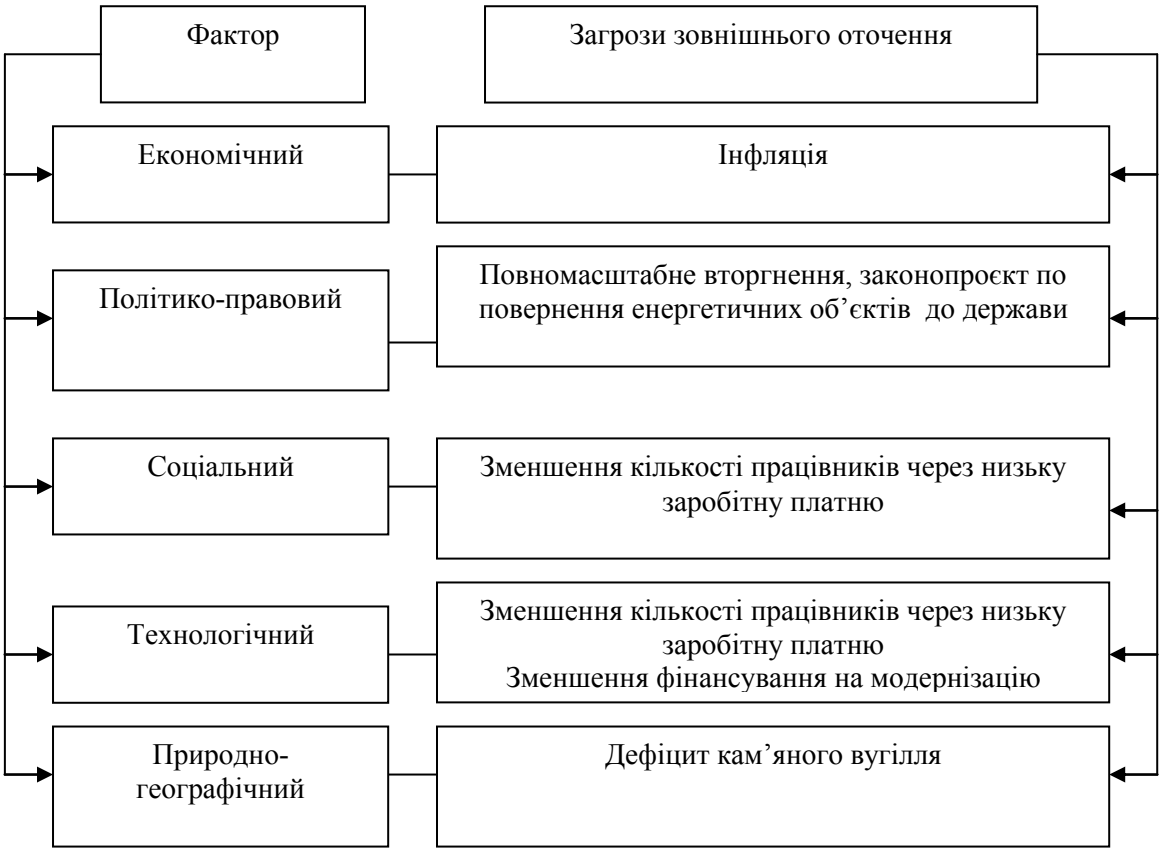


Рис. 2.4. Загрози зовнішнього та внутрішнього оточення для ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ»

- з розвитком новітніх технологій ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» оновлює старе обладнання та автоматизує процеси управління підприємством.

Здійснивши оцінку зовнішнього та внутрішнього середовища ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» можна проаналізувати основні чинники, які здійснюють вплив на його сильні сторони (рис. 2.5):

Рис. 2.5. Сильні сторони ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ»

Для діагностики фінансово-економічної безпеки на підприємстві використовується 2 види: оперативний, статистичний. Застосувавши рекомендований у методичних вказівках «Організаційне та методичне забезпечення виконання дипломних робіт» [34] підхід щодо визначення рівня економічної безпеки підприємства в розрізі певних складових узагальнимо в все це на рис. 2.6 у вигляді пелюсткової діаграми.

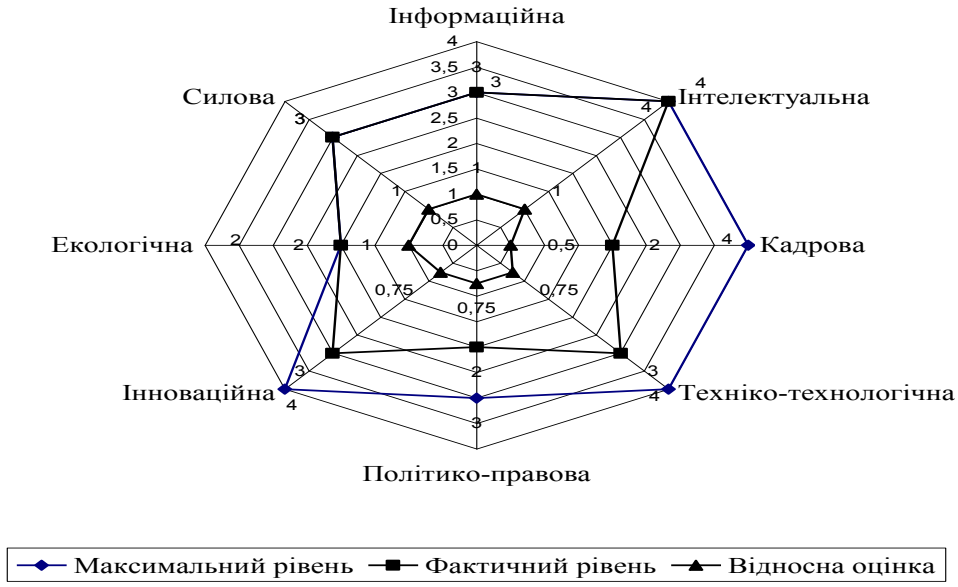


Рис. 2.6. Рівні складових економічної безпеки компанії за 2022 р.

Проаналізувавши складові економічної безпеки підприємства бачимо, що інформаційна, інтелектуальна, екологічна, силова складові на високому рівну. Оцінка 0,5 (кадрова складова) свідчить про ослаблення економічної безпеки підприємства (вище ми зазначали що існують деякі проблеми із зайнятістю, через низьку заробітну платню). Загальний рівень економічної безпеки є задовільний.

Можна зробити загальний висновок, що формування підходів щодо забезпечення економічної безпеки ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» є ключовим питанням сучасного стану розвитку підприємств, формування та вдосконалення систем управління. Компанії необхідно повсякчас думати про адаптацію до реалій сьогодення та здійснювати аналіз ефективних ухвал щодо оптимізації ризиків господарської діяльності.

2.3. Процес управління інформаційною безпекою в ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ»

Створення політики управління інформаційною безпекою є ключовим елементом забезпечення захисту інформації для ПрАТ «ДТЕК

ПАВОГРАДВУГІЛЛЯ». В ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» розроблена політика «Управління інформаційною безпекою технологічної інфраструктури ТОВ ДТЕК ЕНЕРГО», який являється внутрішнім нормативно-правовим документом щодо формування процесу управління у сфері інформаційної безпеки. Політика визначає основні принципи, стандарти та вимоги, які спрямовані на забезпечення конфіденційності, цілісності та доступності даних та інфраструктури

Відмітимо, що управління інформаційною безпекою в ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» належить до компетенції відділу забезпечення інформаційної безпеки - це структура або команда в організації, відповідальна за забезпечення безпеки інформації та технологій. Роль апарату директора з інформаційної безпеки включає в себе розробку та впровадження стратегій і політик інформаційної безпеки, моніторинг та виявлення потенційних загроз, а також взаємодію з іншими відділами для забезпечення відповідності та ефективності заходів з безпеки. Цей апарат складається з інженерів інформаційної безпеки, аналітиків, спеціалістів з кібербезпеки та інших фахівців, які спільно працюють для забезпечення комплексного захисту інформації та технологій (рис. 2.7).

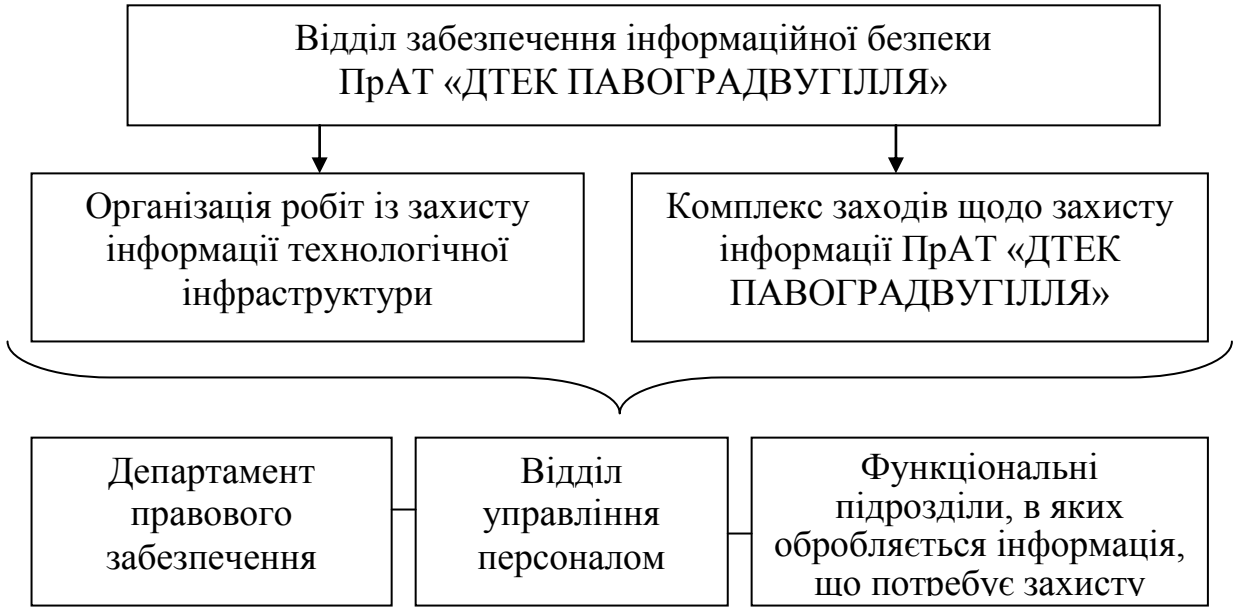


Рис. 2.7. Організаційна структура щодо управління інформаційною безпекою в ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ»

Основні обов’язки та функції апарату директора з інформаційної безпеки включають (рис. 2.8).

Рис. 2.8. Основні обов’язки та функції відділу забезпечення інформаційної безпеки ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ»

Організація робіт із захисту інформації технологічної інфраструктури є критичним завданням для забезпечення безпеки даних та операцій ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ». Забезпечення інформаційної безпеки на всіх етапах життєвого циклу технологічних систем є важливою стратегічною задачею для запобігання потенційним загрозам та забезпечення надійності інфраструктури. Наведемо основні аспекти інформаційної безпеки на різних етапах життєвого циклу технологічних систем:

1. Проектування. Визначення вимог до інформаційної безпеки вже на

етапі проектування системи. Впровадження принципів безпеки на рівні архітектури системи. Врахування можливих загроз та розробка заходів з їх запобігання.

2. Впровадження. Забезпечення безпеки під час конфігурації та встановлення системи. Налаштування прав доступу та контролю за ними. Впровадження систем моніторингу та виявлення інцидентів безпеки.

3. Експлуатація передбачає забезпечення постійного оновлення та патчінгу систем для усунення вразливостей, моніторинг та аналіз подій для виявлення аномалій або підозрілих активностей, навчання персоналу щодо безпекових процедур та практик.

4. На етапі підтримки та оновлення відбувається проведення аудитів безпеки та оцінка дієвості заходів безпеки, забезпечення постійного оновлення політик та процедур безпеки, вдосконалення системи відповідно до змін у загрозах та технологічному середовищі.

5. Вилучення передбачає виконання процедур безпечного вилучення системи, забезпечення безпеки під час перенесення чи вилучення даних, перевірка та видалення всіх служб та ресурсів, що пов'язані із зняттям системи з експлуатації.

Саме інтеграція заходів з інформаційної безпеки на всіх етапах життєвого циклу технологічних систем допомагає забезпечити сталість та високий рівень захисту в умовах зростаючих загроз інформаційної безпеки ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ».

Забезпечення захисту інформації для підприємств, зокрема ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ», є важливим завданням, оскільки вугільна галузь та енергетичні компанії стають об'єктами підвищеної уваги для зловмисників та кібератак. Інформаційний захист включає в себе широкий спектр заходів та стратегій для забезпечення конфіденційності, цілісності та доступності даних та інфраструктури. Комплекс заходів по відношенню до захисту інформації ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» передбачає такі заходи (рис. 2.9):

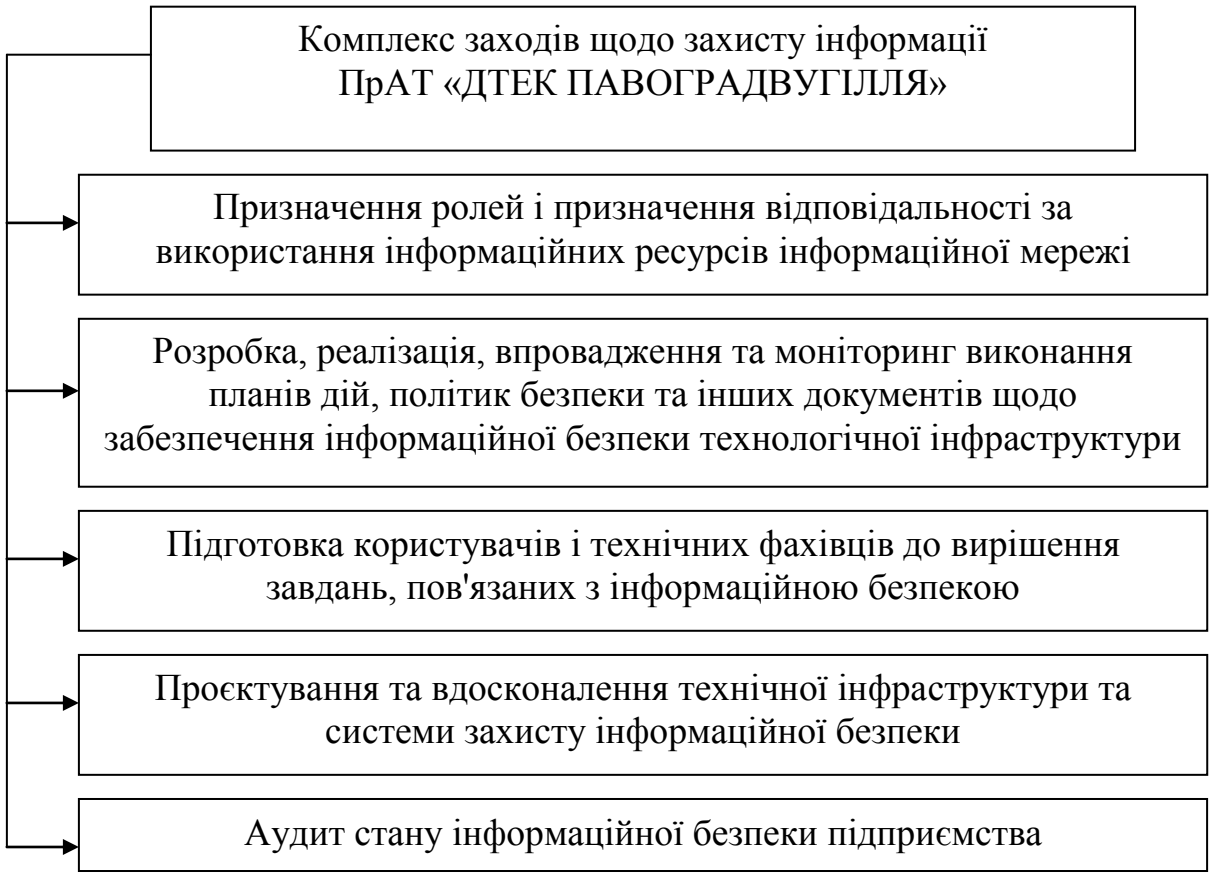


Рис. 2.9. Комплекс заходів щодо захисту інформації ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ»

Відмітимо, що реалізація «Політики забезпечення інформаційної безпеки» ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» здійснюється на підставі затверджених певних програм і планів, які постійно оновлюються з урахуванням динаміки загроз та змін в інформаційному середовищі.

Робота співробітників ВСТІтаІБ (відділу забезпечення інформаційної безпеки) з параметрами безпеки серверів і робочих станцій в промисловій мережі є критично важливою для забезпечення цілісності, конфіденційності та доступності інформації в організації.

Здійснення контролю за налаштуванням параметрів інформаційної безпеки для серверів і робочих станцій промислової мережі є важливим аспектом забезпечення цілісності та безпеки інформації в організації. Основні обов'язки та функції співробітників відділу забезпечення

інформаційної безпеки (ВСТІтаІБ) в цьому контексті включають: визначення стандартів інформаційної безпеки, які визначають необхідні рівні захисту для різних компонентів промислової мережі, визначення стандартів інформаційної безпеки, які визначають необхідні рівні захисту для різних компонентів промислової мережі, узгодження встановлених стандартів та параметрів безпеки зі стейкхолдерами, такими як відділ ІТ, оператори систем, інженери з безпеки тощо, узгодження встановлених стандартів та параметрів безпеки зі стейкхолдерами, такими як відділ ІТ, оператори систем, інженери з безпеки тощо, встановлення та оновлення технічних, організаційних та процедурних заходів інформаційної безпеки відповідно до стандартів, проведення тестувань систем безпеки та перевірка відповідності налаштувань стандартам безпеки, надання навчань та підтримка персоналу щодо правильного використання та налаштування заходів безпеки, розробка планів реагування на інциденти та проведення аналізу інцидентів безпеки, забезпечення виконання політик та встановлених вимог щодо інформаційної безпеки, ведення документації щодо налаштувань та проведення регулярної звітності керівництву. Ці заходи спрямовані на створення ефективного та надійного середовища інформаційної безпеки в промисловій мережі передачі даних.

Висновки до другого розділу

1. ПАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» є частиною вертикально інтегрованої енергетичної Групи ДТЕК і, відповідно, значна частина її продукції продається підприємствам, пов’язаним з ДТЕК. Інтегрований показник фінансового стану за досліджуваний період знаходиться в межах 8,46-8,65 і вказує на досить високий рівень фінансового стану відповідно рейтинг фінансового стану – А. Підхід Групи ДТЕК, до якої належить ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ», до ризик-менеджменту передбачає комплексну систему внутрішнього контролю та управління ризиками,

засновану на стратегічному та поточному плануванні. Функція ризик-менеджменту представлена в ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» як на рівні корпоративного центру, так і на рівні підприємств.

2. Відмітимо, що на підприємстві немає спеціалізованого відділу економічної безпеки, всі обов'язки, пов'язані з забезпеченням економічної безпеки покладені на працівників служби економіки та фінансів. Хоча економічний і фінансовий сектори відіграють важливу роль у цьому процесі, відповідальність за економічну безпеку розподілена між різними функціональними сферами та відділами. Були визначені загрози зовнішнього та внутрішнього оточення для ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ», а також визначені сильні сторони компанії.

3. Проаналізувавши складові економічної безпеки підприємства відмітимо, що інформаційна, інтелектуальна, екологічна, силова складові на високому рівну. Оцінка 0,5 (кадрова складова) свідчить про ослаблення економічної безпеки підприємства (вище ми зазначали що існують деякі проблеми із зайнятістю, через низьку заробітну платню). Загальний рівень економічної безпеки є задовільний. Можна зробити загальний висновок, що формування підходів щодо забезпечення економічної безпеки ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» є ключовим питанням сучасного стану розвитку підприємств, формування та вдосконалення систем управління. Компанії необхідно повсякчас думати про адаптацію до реалій сьогодення та здійснювати аналіз ефективних ухвал щодо оптимізації ризиків господарської діяльності.

4. Створення політики управління інформаційною безпекою є ключовим елементом забезпечення захисту інформації для ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ». В ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» розроблена політика «Управління інформаційною безпекою технологічної інфраструктури ТОВ ДТЕК ЕНЕРГО», який являється внутрішнім нормативно-правовим документом щодо формування процесу управління у сфері інформаційної безпеки. Політика визначає основні принципи,

стандарти та вимоги, які спрямовані на забезпечення конфіденційності, цілісності та доступності даних та інфраструктури.

5. Відмітимо, що управління інформаційною безпекою в ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» належить до компетенції відділу забезпечення інформаційної безпеки - це структура або команда в організації, відповідальна за забезпечення безпеки інформації та технологій. Роль апарату директора з інформаційної безпеки включає в себе розробку та впровадження стратегій і політик інформаційної безпеки, моніторинг та виявлення потенційних загроз, а також взаємодію з іншими відділами для забезпечення відповідності та ефективності заходів з безпеки. Цей апарат складається з інженерів інформаційної безпеки, аналітиків, спеціалістів з кібербезпеки та інших фахівців, які спільно працюють для забезпечення комплексного захисту інформації та технологій.

6. Забезпечення захисту інформації для підприємств є важливим завданням, оскільки вугільна галузь та енергетичні компанії стають об'єктами підвищеної уваги для зловмисників та кібератак. Інформаційний захист включає в себе широкий спектр заходів та стратегій для забезпечення конфіденційності, цілісності та доступності даних та інфраструктури, а саме: визначення відповідальності за використання інформаційних ресурсів; розробка, реалізація, впровадження та моніторинг виконання планів дій, щодо забезпечення інформаційної безпеки; підготовка користувачів і технічних фахівців до вирішення завдань, пов'язаних з інформаційною безпекою; проєктування та вдосконалення системи захисту інформаційної безпеки; аудит стану інформаційної безпеки підприємства.

РОЗДІЛ 3. ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1. Проблеми та перспективи щодо управління інформаційною безпекою

Вислів Вінстона Черчілля «Хто володіє інформацією, той володіє світом» чудово відображає сутність важливості інформації в сучасному світі. В інформаційному суспільстві, де технології і обмін даними стали необхідною частиною кожного аспекту життя, захист інформації стає критично важливим завданням.

Безпека інформаційних систем стає частиною основного бізнесу в кожній організації, кожному підприємстві. В сучасному бізнес-середовищі безпека інформаційних систем стала необхідною складовою успішної діяльності будь-якої організації чи підприємства [33]. Інформаційні системи використовуються для зберігання, обробки та обміну великої кількості даних, включаючи конфіденційну і критично важливу інформацію. Інформаційна безпека передбачає заходи для забезпечення конфіденційності, цілісності та доступності інформації. Захищена інформація важлива для бізнесу, влади, науки, освіти та інших сфер. Забезпечення інформаційної безпеки стає завданням як на рівні окремих організацій, так і на рівні національної та міжнародної безпеки.

Інформаційна безпека включає в себе різноманітні аспекти, такі як захист від кіберзагроз, керування доступом до даних, розробка та дотримання політик безпеки, аудит безпеки, та багато інших. Збереження конфіденційності та цілісності даних, а також забезпечення їх доступності у відповідності з встановленими стандартами та законодавством, стає важливою складовою успішної діяльності будь-якої організації чи країни.

Керівництво підприємства стикається з рядом важливих проблем у сфері інформаційної безпеки (рис. 3.1):

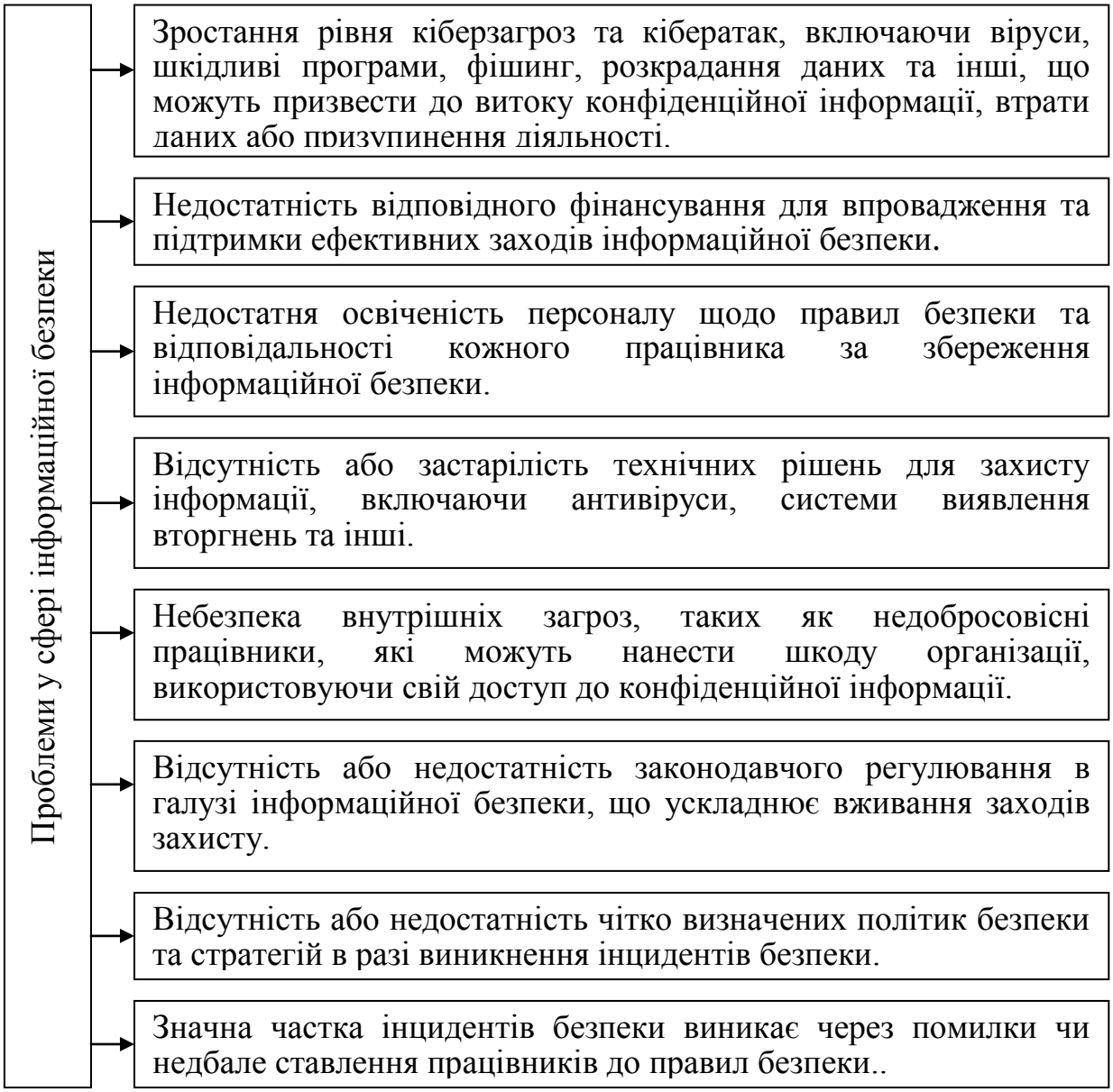


Рис. 3.1. Проблеми у сфері інформаційної безпеки

Якщо ми хочемо досягнути довготривалого ефекту, то розв’язання цих проблем вимагає не фрагментарного, а комплексного підходу, включаючи інвестиції в технології, освіту персоналу, розробку політик і планів безпеки, а також ефективне управління ризиками. Такий підхід дозволяє створити міцну систему захисту інформації, що враховує технології, людей і процеси, і забезпечує ефективний відгук на сучасні виклики в області інформаційної

безпеки.

Пропонуємо розглянути напрями технічного захисту інформаційного середовища підприємства є (рис. 3.2):

Рис. 3.2. Напрями технічного захисту
інформаційного середовища підприємства

Відмітимо, що управління інформаційною безпекою складається із зобов'язань керівництва, організаційних структур, обізнаності та зобов'язань користувачів, політик, процедур, процесів, технологій та механізмів забезпечення відповідності, які працюють разом, щоб забезпечити конфіденційність, цілісність і доступність електронних активи компанії.

Крім того, управління інформаційною безпекою є обов'язком виконавчого керівництва. Управління інформаційною безпекою має також гарантувати належне пом'якшення ризиків економічно ефективним способом, отже, можна розглядати як підтримку управління ризиками, і, таким чином, відповідним способом захищати розраховані ризики.

Інформація є активом, необхідним для діяльності організації, і, отже, її потрібно належним чином захищати. Метою інформаційної безпеки є забезпечення безперервності бізнесу та мінімізація збитків для бізнесу шляхом обмеження впливу інцидентів безпеки [37].

Міжнародний стандарт ISO/IEC 27002 визначає інформаційну безпеку як захист інформації від широкого спектру загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес-ризику та максимізації прибутку від інвестицій і бізнес-можливостей [46]. Крім того, ISO/IEC 27002 пояснює, що для досягнення інформаційної безпеки необхідно запровадити набір засобів контролю, включаючи політики, процеси, процедури, організаційні структури та функції програмного та апаратного забезпечення. Ці засоби контролю необхідно встановлювати, впроваджувати, контролювати, переглядати та вдосконалювати, де це необхідно, щоб гарантувати виконання конкретних цілей безпеки та бізнесу організації.

Також інформаційна безпека це захист інформаційних активів, які використовують, зберігають або передають інформацію, від ризику шляхом застосування політики технологій. Окрім цього, критичні характеристики інформації, серед яких конфіденційність, цілісність і доступність, повинні бути захищені в будь-який час, цей захист реалізується за допомогою багатьох заходів.

Інформація та допоміжні процеси, системи та мережі є важливими бізнес-активами [49]. Визначення, досягнення, підтримка та покращення інформаційної безпеки може мати важливе значення для підтримки конкурентоспроможності, грошового потоку, прибутковості, дотримання законодавства та комерційного іміджу. Як пояснювалося раніше, організації

стикаються із загрозами з різних джерел, які, як наслідок, становлять ризик для загального добробуту організації.

Багато ІТ-систем розроблено не для забезпечення безпеки, а для досягнення своєї головної мети, наприклад, головна мета принтера — надрукувати документ, а не гарантувати відсутність шпигунства під час виконання своїх операцій. Безпека, яку можна досягти за допомогою технічних засобів, обмежена, і її слід підтримувати відповідним управлінням і процедурами. Визначення того, які засоби контролю слід застосовувати, вимагає ретельного планування та уваги до деталей. Інформаційна безпека повинна практикуватися всіма співробітниками підприємства, а також може включати треті сторони, постачальників і навіть клієнтів.

Саме управління інформаційною безпекою забезпечує дотримання цих практик інформаційної безпеки та гарантує дотримання належного рівня відповідності. Пропонуємо розглянути загальний підхід до управління інформаційною безпекою (рис. 3.3).

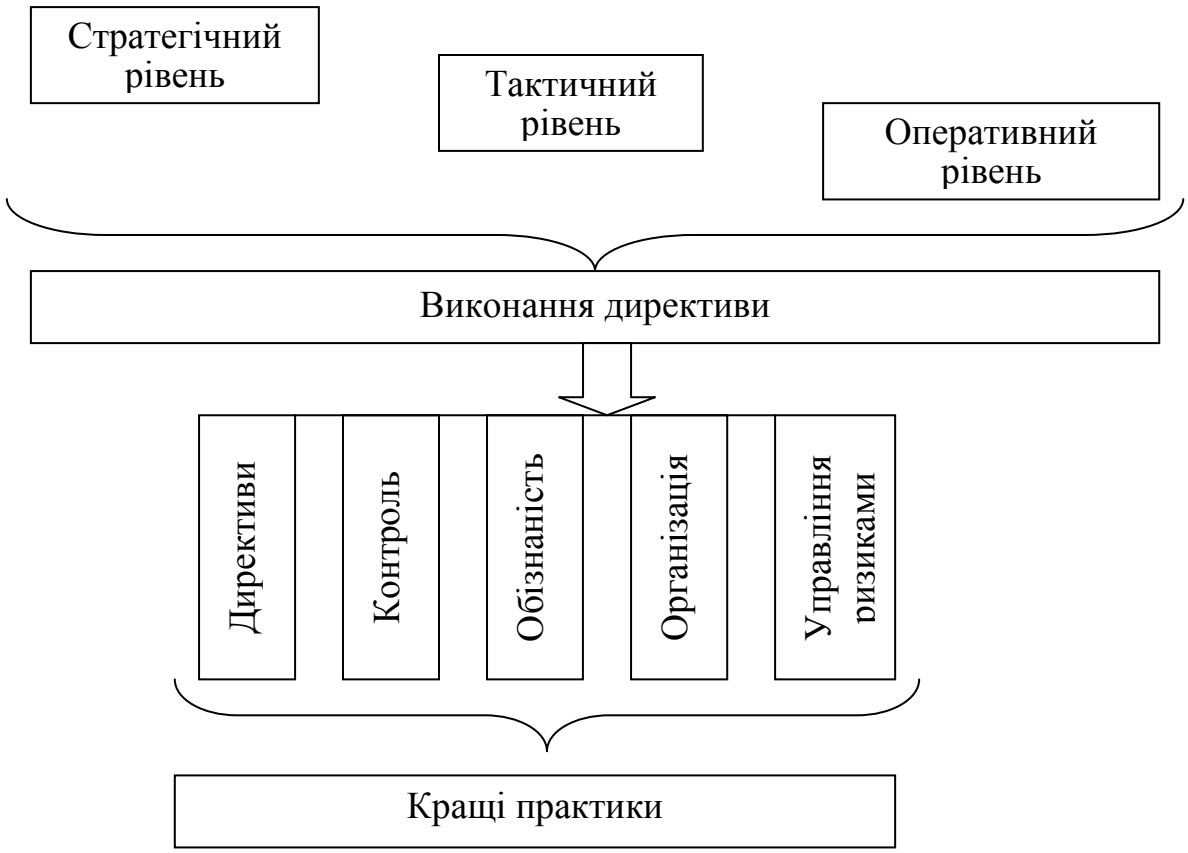


Рис. 3.3. Загальний підхід до управління інформаційною безпекою

Даний підхід складається із базису (серцевини) і ряду глибинних розмірів. Зауважимо, що розміри глибини представляють лише деякі розміри, зокрема: директиви, контроль, аспект управління ризиками, організаційний вимір, вимір обізнаності.

Проте, можемо відмітити, що, в принципі, модель також повинна охоплювати більше вимірів, а саме: політичний вимір, вимір сертифікації, етичний вимір, правовий/нормативний аспект, страховий вимір, розмір вимірювання, моніторингу, управлінський вимір, технічний вимір.

Основна частина моделі ілюструє види управління [54]:

- стратегічний рівень (рада та виконавче керівництво вирішують, що потрібно зробити);

- тактичний рівень (вище та середнє керівництво вирішує, як це робити);

- операційний рівень (нижчий рівень управління та адміністрування, де виконуються визначені директиви).

На першому рівні рада та виконавче керівництво повинні визначити, наскільки важливими вони бачать інформаційні активи компанії та який вплив вони мають на стратегічне бачення підприємства. Тому Правління має вказати, наскільки важливо захистити ці активи. Такі рішення ґрунтуються на таких факторах, як: зовнішні фактори, такі як правові та нормативні приписи та зовнішні ризики та внутрішні чинники, такі як стратегічне бачення підприємства, роль ІТ на підприємстві, узгодження ІТ зі стратегією підприємства, конкурентоспроможність тощо. Результатом таких обговорень стане набір директив, які на високому рівні вказуватимуть на те, що Рада очікує, що має бути зроблено для захисту добробуту підприємства. Тепер ці директиви стають входом до тактичного рівня управління.

На тактичному рівні директиви, що надходять зі стратегічного рівня, діють як вхідні дані для управління на тактичному рівні. Потім ці директиви розширюються до наборів відповідних політик інформаційної безпеки, процедур і стандартів компанії. Результатом цього рівня є набір документів,

які пояснюють, як використовувати директиви для операційного рівня.

Вхідними даними для операційного рівня є набір політик, стандартів і процедур, створених на попередньому рівні управління. На операційному рівні ці документи знову розширюються, щоб створити набір адміністративних вказівок і процедур. Тепер ці документи відображають оперативні процедури і повинні використовуватися як основа для виконання на найнижчому рівні.

До цього часу було показано, як процес управління інформаційною безпекою спрямовується зверху вниз до найнижчого рівня. Зауважте, що директиви зверху вниз зростають від верху до низу, вказуючи на те, що директиви вгорі короткі та високі. Це вказує на те, що директиви стають дедалі деталізованішими та заповненими, оскільки директиви високого рівня розширюються на кожному нижчому рівні.

Щоб виміряти відповідність встановленим директивам, частина моделі «Контроль» вказує, як це має виконуватися. Контрольна частина також виникає на всіх трьох рівнях управління [57]. Наприклад, на операційному рівні дані вимірювань беруться з різних джерел. Це вилучення може бути здійснено в електронному вигляді, наприклад, з файлів журналів, баз даних, брандмауерів тощо. Деякі дані, які не можуть бути отримані в електронному вигляді, збираються за допомогою інтерв'ю, анкет, перевірок тощо. На основі зібраних даних формується звіт, який передається на тактичний рівень управління.

На тактичному рівні оперативні дані вимірювань збираються та інтегруються для виконання вимірювань і моніторингу відповідно до вимог відповідної політики, процедур та стандартів. Формуються звіти із зазначенням рівня відповідності, які надаються керівництву стратегічного рівня.

Тепер показано, як процес управління інформаційною безпекою контролюється шляхом звітування про відповідність знизу вгору. Зауважимо, що напрям дії вгору зменшується в розмірі, вказуючи на те, що звіти внизу

більш детальні, тоді як звіти стають менш детальними, коли процес просувається вгору по рівнях. Це свідчить про те, що звітність поступово стає менш детальною та високорівневою.

Звертаємо увагу, що найкращі практики формують основу, що впливає на всі інші виміри. Метою цього виміру в моделі є надання вказівок щодо того, як потрібно звертатися до кожного з основних вимірів. Політика інформаційної безпеки розглядається як звичайна практика та важливий компонент будь-якого плану інформаційної безпеки. Без політики впорядкування не має змісту та правил, які слід її забезпечити. Керівництво має гарантувати, що розроблена політика інформаційної безпеки підтримується в цілому по підприємству.

У цьому розділі пояснюється пряма частина моделі, показуючи, як директиви розширюються зі стратегічного рівня на тактичний і оперативний рівень. Буде пояснено процес формування політик, процедур і стандартів, а також зв’язок із корпоративною політикою інформаційної безпеки.

Зазначимо, що необхідно розробити певну систему нормативних документів, які безпосередньо будуть регулювати процес управління інформаційною безпекою підприємства [3]:

- ініційована правлінням директива щодо управління інформаційною безпекою;

- корпоративна політика інформаційної безпеки, що випливає з директиви;

- набір детальних підполітик, що випливають із корпоративної політики інформаційної безпеки;

- набір стандартів компанії на основі корпоративної та детальної політики;

- набір адміністративних та операційних процедур, які знову ж таки випливають із детального набору підполітик.

Крім того, ці документи структуровані таким чином, щоб сформувати архітектуру політики інформаційної безпеки.

Директива правління є найвищим рівнем ієрархії та має вказувати на важливість активів підприємства з обробки інформації. Крім того, у ньому має бути зазначено повноваження ради захистити ці активи. Директиви правління не обов'язково повинні бути повністю присвячені інформаційній безпеці, але вони повинні містити достатньо змісту, щоб спонукати та мотивувати створення та існування Політики корпоративної інформаційної безпеки.

Політика корпоративної інформаційної безпеки (ПКІБ) - це документ високого рівня, який є основою для всіх документів нижчого рівня, пов'язаних із інформаційною безпекою. Вони включають наступне:

- ПКІБ має вказувати на підтримку та зобов'язання правління та виконавчого керівництва, і має бути чітко зазначено, що ПКІБ випливає з директиви вищого рівня;

- ПКІБ має бути прийнятою і підписаною генеральним директором або іншою уповноваженою посадовою особою;

- ПКІБ не повинна бути довгою не повинен бути написаною у технічному форматі. Вона має містити бачення високого рівня щодо інформаційної безпеки;

- ПКІБ не повинна змінюватися дуже часто і повинна бути стабільною, що стосується технічних розробок і змін.

Набір загальних підполітик може відрізнятися від компанії до компанії на основі корпоративної політики безпеки інформації, як пояснено вище. Однак деякі політики є загальними, наприклад: політика контролю шкідливого програмного забезпечення (антивірусна політика); прийнятна політика використання Інтернету; прийнятна політика використання електронної пошти; політика логічного контролю доступу; політика аварійного відновлення (резервне копіювання); політика контролю віддаленого доступу; політика контролю доступу третіх сторін.

Що важливо, так це те, що кожна з цих підполітик повинна мати положення про відповідність. Кожна з цих підполітик потім розширюється,

щоб сформувати набір процедур, щоб пояснити, як усе має відбуватися на операційному рівні.

3.2. Методичний підхід до управління ризиками інформаційної безпеки

Управління ризиками інформаційної безпеки - це процес визначення, аналізу, оцінювання та зменшення потенційних загроз та вразливостей, пов'язаних з інформаційною безпекою. Метою цього процесу є забезпечення конфіденційності, цілісності та доступності інформації, а також запобігання втратам даних та ризикам для бізнес-процесів. Ефективне управління ризиками інформаційної безпеки дозволяє організації адекватно відповідати на потенційні загрози і забезпечити стійкість її інформаційної інфраструктури.

Комплексний погляд на управління ризиками інформаційної безпеки означає, що організаційні проблеми, людські фактори та вплив навколишнього середовища також прямо чи опосередковано впливають на результати управління ризиками безпеки.

Ретельне дослідження основних застосованих підходів до управління ризиками інформаційної безпеки підкреслило потребу в новій комплексній структурі управління ризиками інформаційної безпеки, яка дає змогу підприємствам ефективно та результативно розглядати всі аспекти управління ризиками інформаційної безпеки [11]. Таким чином, структура управління ризиками інформаційної безпеки повинна враховувати такі основні вимоги:

- включати основні елементи методики управління ризиками;

- володіти всеосяжним обсягом, який не лише обмежує аналіз управління ризиками інформаційної безпеки до технічних питань, але також включає питання організації, людей та навколишнього середовища;

- залежить від процесу управління, який об’єднує основні підходи до управління ризиками інформаційної безпеки та містить основні компоненти

методики управління ризиками;

- кількісно оцінити поточну ситуацію з інформаційною безпекою підприємства, використовуючи дійсну та надійну техніку моделювання.

- основу вибору рекомендованих заходів безпеки ISO/IEC 27002 на основі економічного аналізу.

На додаток до попередніх основних вимог, чітко визначена політика інформаційної безпеки, навчена команда підтримки зсередини підприємства та чітке визначення термінів і концепцій управління ризиками відіграють вирішальну роль в успішній розробці ефективної структури управління ризиками інформаційної безпеки.

Більшість методологій управління інформаційними ризиками зосереджені в основному на технологічних рішеннях і ще не повністю запровадили комплексний підхід, який розглядає організаційні, людські та екологічні фактори при вивченні проблем інформаційної безпеки.

Волот О. [12] обговорює дисбаланс простору проблеми безпеки. Вони помітили, що понад 94% публічних досліджень комп'ютерної безпеки були зосереджені лише на технологічних факторах. Чанг і Хо [57] досліджує вплив організаційних факторів на впровадження системи управління інформаційною безпекою. Результати показують прямий вплив організаційних факторів на ефективне впровадження стандарту щодо інформаційної безпеки. Чубаєвський В., Жук Т. [52] вивчають вплив людських та організаційних факторів на комп'ютерну та інформаційну безпеку. Вони довели, що людські та організаційні фактори відіграють значну роль у розвитку вразливостей комп'ютерної та інформаційної безпеки. Ракіпов В.Р.[42] пропонує інтегровану структуру для розгляду людських, організаційних і технологічних проблем управління IT-безпекою.

Система управління - це структура процесів і процедур, які використовуються для забезпечення того, щоб підприємство могло виконувати всі завдання, необхідні для досягнення його цілей. Основна мета системи управління полягає в постійному вдосконаленні підприємства у

відповідній сфері. Наведений вище огляд показує, що кожен із розглянутих методів управління ризиками використовує власну систему управління під час здійснення процесу управління ризиками.

Система управління залежить від процесу плануй, роби, перевіряй і дій (PDCA) для створення, впровадження, експлуатації, моніторингу, перегляду, підтримки та вдосконалення системи управління інформаційною безпекою будь-якого підприємства. Концепція моделі PDCA була спочатку розроблена в 1930 році Уолтером Шухартом. Концепція PDCA була підхоплена та дуже ефективно пропагована з 1950-х років У. Едвардсом Демінгом, і тому відома багатьом як «колесо Демінга». Застосування PDCA для управління ризиками інформаційної безпеки представлено в табл. (3.1).

Таблиця 3.1

Процес управління ризиками інформаційної безпеки

Складові	Пояснення
План	Встановіть контекст. Оцінка ризику. Розробка плану «лікування ризику». Прийняття ризику.
Виконання	Впровадження плану «лікування» ризиків.
Перевірка	Постійний моніторинг та аналіз ризиків.
Впровадження (дія)	Підтримувати та вдосконалювати процес управління ризиками інформаційної безпеки

Застосуванню моделі PDCA в процесі управління ризиками бракує справедливого узгодження діяльності з управління ризиками. Очевидно, що наукове походження PDCA «гіпотеза, експеримент і оцінка» перешкоджає його здатності належним чином охоплювати діяльність з управління ризиками.

У стандарті ISO/IEC 27004 зазначено, що для того, щоб надати вищому керівництву переконливі аргументи для ініціювання програми інформаційної безпеки, спеціалісти з інформаційної безпеки повинні визначити ризики для організаційних процесів [46]. Стандарт також пропонує розробити систему

вимірювання, здатну визначати ефективність засобів контролю, запроваджених відповідно до додатку А стандарту ISO/IEC 27001. Потреба в нових методах для оцінки ефективного використання ISO/IEC 27002 для захисту інформаційних ресурсів є важливим. Політанський В.С.[39] наголосив на необхідності адекватної системи вимірювання зрілості для практики управління інформаційною безпекою.

Правдивець О. [40] оцінив ефективність управління інформаційною безпекою на основі методики вимірювання, яка включає охоплення бізнес-процесу, оперативність засобів контролю та повноту політики безпеки. Марущак А. [30] зазначив, що сертифікація може дати підприємствам помилкове відчуття безпеки. Він запропонував підприємствам розробити та впровадити систему вимірювання інформаційної безпеки, яка внутрішньо оцінює готовність їхніх заходів захисту інформаційної безпеки.

Однією з важливих вимог у розробці ефективної структури управління ризиками інформаційної безпеки є визначення відповідної стратегії для створення політики інформаційної безпеки підприємства. Ця політика повинна ґрунтуватися на міжнародних стандартах інформаційної безпеки та мати безперервний характер, щоб розвиватися зі змінами сфери інформаційної безпеки. Крім того, залучення навченої команди, що складається з власників системи, зберігачів і користувачів відповідного підприємства, у процесі планування, розробки та реалізації програм управління ризиками інформаційної безпеки є важливим фактором для успіху цих програм.

На нашу думку, методичний підхід до управління ризиками інформаційної безпеки, який базується на систематичному та структурованому підході до виявлення, аналізу та управління ризиками та передбачає (рис. 3.4). Цей методичний підхід дозволяє створити системний підхід до управління ризиками інформаційної безпеки та постійно підтримувати безпековий стан підприємства.

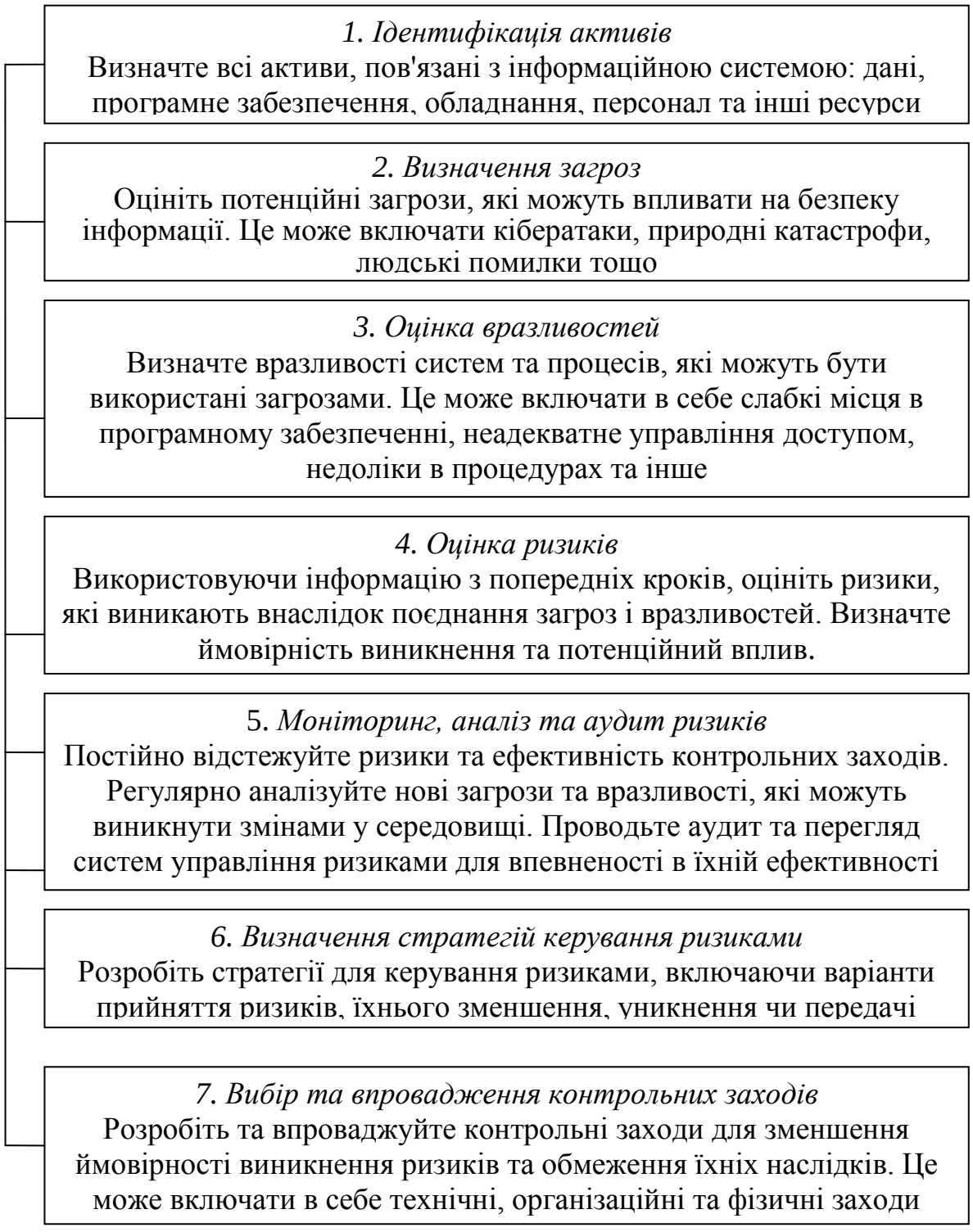


Рис. 3.4. Основні складові методичного підходу до управління ризиками інформаційної безпеки

Відповідно до визначеного методичного підходу до управління ризиками інформаційної безпеки можемо запропонувати алгоритм взаємодії елементів процесу щодо управління ризиками інформаційної безпеки

(додаток Ж). Цей комплексний підхід дозволяє створити міцну систему захисту інформації, що враховує технології, людей і процеси, і забезпечує ефективний відгук на сучасні виклики в області інформаційної безпеки.

Таким чином, управління ризиками інформаційної безпеки підприємства, професійних і дослідницьких методів полягає в тому, що вони надають різні інструменти та методи для досягнення загалом однієї мети захисту інформаційних ресурсів підприємства шляхом визначення відповідних заходів захисту безпеки за допомогою підходів до управління ризиками. Однак ці методи досягають цієї мети за допомогою різних підходів: підходу аналізу ризику та підходу найкращої практики, і мають різні рівні, деякі методи є високорівневими лише для надання вказівок, тоді як інші є більш детальними та зосереджені головним чином на досягненні кращого аналізу ризиків результати. Більшість доступних методів управління ризиками мають технічний характер та ігнорують оцінку поточного стану інформаційної безпеки підприємства. Крім того, ці методи не залежать від стандартного економічного підходу до вибору відповідних засобів захисту безпеки. Кожен метод має свої сильні та слабкі сторони, і вважається, що інтеграція цих методів у еталонну комплексну структуру управління ризиками інформаційної безпеки підприємства дозволить досягти кращих результатів.

3.3. Економіко-математичні методи та моделі в управлінні інформаційною безпекою для забезпечення економічної безпеки підприємства

Управління інформаційною безпекою в контексті забезпечення економічної безпеки підприємства є досить важливими в сучасних умовах, оскільки інформаційні технології стають неодмінною частиною діяльності більшості підприємств України. Забезпечення ефективної інформаційної безпеки стає важливим аспектом економічного успіху та стійкості підприємства, тому актуальним є питання удосконалення управління

інформаційною безпекою в контексті забезпечення економічної безпеки підприємства.

Пропонуємо звернути увагу на деякі ключові аспекти управління інформаційною безпекою [35]:

1. Визначення інформаційної безпеки: інформаційна безпека визначається як забезпечення конфіденційності, цілісності та доступності інформації.

2. Загрози інформаційній безпеці: розгляд та аналіз потенційних загроз, таких як кібератаки, витоки даних, внутрішні загрози та інші.

3. Ролі управління інформаційною безпекою: зазначення ролі та відповідальності керівництва, IT-персоналу та всіх працівників у забезпеченні інформаційної безпеки.

4. Системи управління інформаційною безпекою (СУІБ): огляд різних методів та стандартів для впровадження СУІБ на підприємствах, таких як ISO/IEC 27001.

5. Економічні витрати на інформаційну безпеку: розгляд витрат на заходи з підвищення інформаційної безпеки та їх вплив на економічну діяльність підприємства.

6. Практика та кейси: аналіз конкретних прикладів успішного управління інформаційною безпекою на підприємствах.

7. Напрями вдосконалення: обговорення новітніх тенденцій та стратегій для поліпшення інформаційної безпеки, включаючи використання штучного інтелекту, блокчейну та інших інноваційних технологій.

8. Законодавство та нормативи: перегляд правових вимог та стандартів, які регулюють сферу інформаційної безпеки.

Кожен такий аспект, сам по собі, не може значно вплинути на інформаційну безпеку підприємства. Тільки комплексний підхід та поєднання технічних, організаційних та правових заходів дає можливість забезпечення повного циклу інформаційної безпеки на підприємстві. Особливу роль в управлінні інформаційною безпекою займають математичні

методи та елементи економіко-математичного моделювання. Цей підхід використовують для аналізу і вдосконалення різних аспектів інформаційної безпеки та їх впливу на економіку підприємства. Ось деякі приклади застосування економіко-математичних моделей:

1. Оцінка ризиків - використання статистичних методів та ймовірнісних моделей для оцінки ризиків інформаційної безпеки [34]. Це дозволяє керівництву підприємства приймати рішення з врахуванням ймовірних наслідків інцидентів і розробляти стратегії для їх зменшення.

2. Оптимізація бюджету інформаційної безпеки - розробка математичних моделей для оптимізації розподілу бюджету на заходи із забезпечення інформаційної безпеки. Це допомагає визначити оптимальні витрати для максимізації ефективності заходів з безпеки.

3. Моделювання стратегій відновлення: використання математичних моделей для моделювання різних стратегій відновлення після інцидентів і забезпечення максимальної ефективності при використанні обмежених ресурсів [23].

4. Аналіз вартості інцидентів - розрахунок економічних збитків від інцидентів із застосуванням математичних моделей. Це може включати оцінку втрат у виробництві, втрати клієнтів та репутаційні втрати.

5. Оптимізація процесів управління інформаційною безпекою - розробка оптимальних математичних моделей для управління процесами інформаційної безпеки, враховуючи внутрішні та зовнішні чинники.

6. Моделювання впливу стратегій безпеки на фінансові показники: використання математичних моделей для аналізу впливу заходів з інформаційної безпеки на фінансовий стан підприємства, враховуючи вартість впровадження та очікувані вигоди.

Отже, застосування економіко-математичних моделей дозволяє підприємствам більш раціонально розуміти витрати та ефективність заходів з інформаційної безпеки, сприяючи вирішенню важливих завдань у контексті економічної безпеки.

Розглянемо приклад математичної моделі для оптимізації процесів управління інформаційною безпекою, зосереджуючись на вирішенні проблеми призначення ресурсів для заходів з інформаційної безпеки. В загальному вигляді математична модель буде мати наступний вид:

Нехай є наступні змінні, які мають наступні позначки:

– x_i - обсяг ресурсів, виділених для заходів з інформаційної безпеки на підприємстві.

– $C_i(x_i)$ - функція вартості заходів з інформаційної безпеки на підприємстві, яка залежить від обсягу виділених ресурсів.

– $E_i(x_i)$ - функція ефективності заходів з інформаційної безпеки на підприємстві, яка також залежить від обсягу виділених ресурсів.

– $R_i(x_i)$ - рівень ризику на підприємстві, що також залежить від обсягу виділених ресурсів.

Тоді сформулювати задачу оптимізації можна наступним чином:

$$J(x) = \sum_{i=1}^{N} C_i(x_i) \to min \cdot$$

при умові, що обмеження будуть мати вид

$$\sum_{i=1}^{N} E_i(x_i) \geq E_{\min} \square ,$$

$$\sum_{i=1}^{N} R_i(x_i) \geq R_{\max} \square ,$$

де $J(x)$ – загальні витрати на заходи з інформаційної безпеки;

E_{min} - мінімально прийнятний рівень ефективності заходів;

R_{max} - максимально прийнятний рівень ризику.

Така модель дозволяє підприємству знайти оптимальний розподіл ресурсів між різними заходами з інформаційної безпеки, забезпечуючи заданий рівень ефективності та обмежуючи рівень ризику. Можна використовувати числові методи оптимізації, такі як методи градієнтного спуску або еволюційні алгоритми, для знаходження оптимального рішення. Цей приклад лише ілюструє загальний підхід до використання математичних

моделей у сфері управління інформаційною безпекою, і конкретні функції вартості, ефективності та ризику повинні бути адаптовані до конкретних умов та конкретних потреб підприємства.

Крім того, можуть бути застосовані статистичні методи та ймовірннісні моделі окремо для оцінки ризиків (рис. 3.5) інформаційної безпеки. Це дозволить керівництву підприємства приймати рішення з врахуванням ймовірних наслідків інцидентів і розробляти стратегії для їх зменшення.

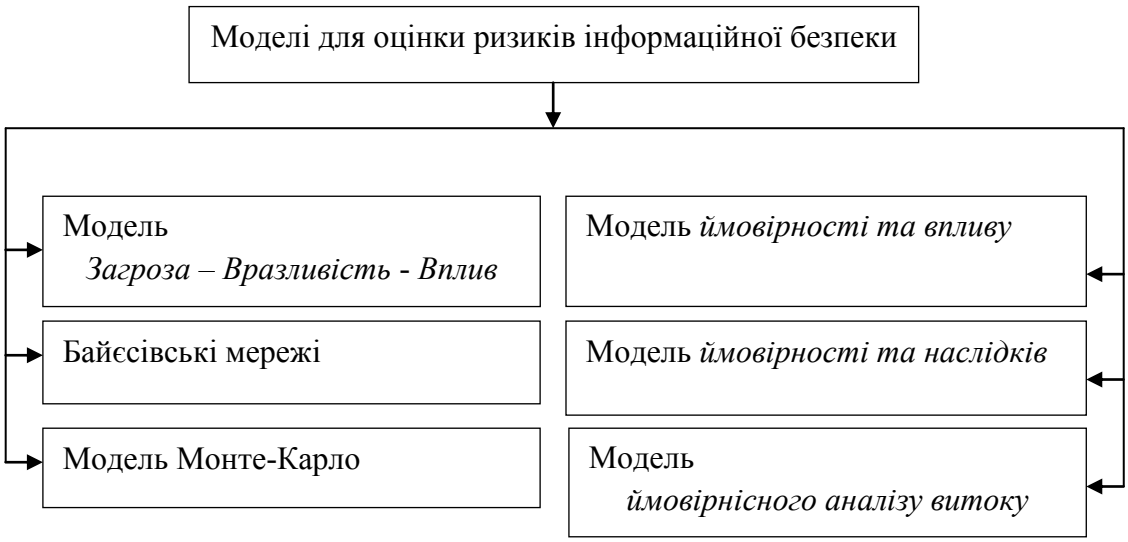


Рис. 3.5. Методи та моделі для оцінки ризиків

Наведені моделі можна адаптувати в залежності від конкретних потреб та характеристик підприємства. Вони допомагають керівництву приймати обґрунтовані рішення та розробляти стратегії для зменшення ймовірності та наслідків інцидентів інформаційної безпеки.

Щоб детальніше проаналізувати розвиток та функціонування діяльності ПрАТ ДТЕК «ПАВЛОГРАДВУГІЛЛЯ» необхідно скласти економіко-математичну модель, яка включає у себе фактори економічної безпеки, витрати на інформаційну безпеку та інше. Для підприємства ПрАТ ДТЕК «ПАВЛОГРАДВУГІЛЛЯ» таким типом моделі будемо використовувати модель оптимізації системи інформаційної безпеки. Необхідно мінімізувати ризики та витрати на інформаційну безпеку при забезпеченні оптимального рівня захисту.

Розглянемо задачу лінійного програмування, в якій необхідно оптимально розподілити бюджет (4368863 грн) з різними заходами з інформаційної безпеки. Дані для моделі в таблиці 3.2.

Таблиця 3.2

Числові дані ПрАТ ДТЕК «ПАВЛОГРАДВУГІЛЛЯ» для оптимізаційної моделі

Заходи з інформаційної безпеки	Вартість заходів з інформаційної безпеки, грн	Максимальні ризики	Мінімальні вимоги до безпеки
Захист від несанкціонованого доступу до даних підприємства	2520	0,05	0,02
Аудит безпеки підприємства	4800	0,03	0,01
Захист мережі підприємства	3360	0,08	0,03
Навчання персоналу підприємства	950	0,04	0,015
Моніторинг безпеки підприємства	1080	0,07	0,025

Економіко-математична модель з даними:

Цільова функція

$$0{,}05 \cdot x_1 + 0{,}03 \cdot x_2 + 0{,}08 \cdot x_3 + 0{,}04 \cdot x_4 + 0{,}07 \cdot x_5 \rightarrow min$$

Обмеження:

$$2520 \cdot x_1 + 4800 \cdot x_2 + 3360 \cdot x_3 + 950 \cdot x_4 + 1080 \cdot x_5 \leq 4368863$$

$$0{,}02 \cdot x_1 + 0{,}01 \cdot x_2 + 0{,}03 \cdot x_3 + 0{,}015 \cdot x_4 + 0{,}025 \cdot x_5 \geq 0{,}03$$

$$x_1 \geq 0, x_2 \geq 0, x_3 \geq 0, x_4 \geq 0, x_5 \geq 0$$

Отримали звичайну задачу лінійного програмування, яку розв’язати з використанням сиплексного методу (що є складним при збільшенні кількості змінних), з використанням спеціалізованих надбудов електронних таблиць Microsoft Excel (додаток З) або з підключенням та застосуванням бібліотек для мови програмування Python, яка називається PuLP (бібліотека PuLP

автоматично визначає оптимальний розподіл бюджету для мінімізації ризиків за заданих обмежень).

У табл. 3.3 наведені результати розрахунків за побудованою моделлю та варіанти ступеня ризику.

Таблиця 3.3

Варіанти розрахунків за оптимізаційною моделлю

Заходи з інформаційної безпеки	Варіант 1	Варіант 2	Варіант 3
Захист від несанкціонованого доступу до даних підприємства	0,037	0,035	0,034
Аудит безпеки підприємства	0,018	0,017	0,017
Захист мережі підприємства	0,039	0,036	0,034
Навчання персоналу підприємства	0,015	0,013	0,012
Моніторинг безпеки підприємства	0,03	0,028	0,025
Фактичні витрати на заходи з інформаційної безпеки	3152758	3867378	4052748
Максимально прийнятний рівень ризику	0,082	0,071	0,069

Результати розрахунків у табл. 3.3 свідчать про те, що економічний ризик на ПрАТ ДТЕК «ПАВЛОГРАДВУГІЛЛЯ» можна за відповідних заходів управління інформаційною безпекою значно знизити.

Модель можливо модифікувати, а саме, додати заходи з інформаційної безпеки, змінити критерії, додати обмеження, змінити граничні рівні змінних, ризику та інше. Засоби інформаційних технологій електронних таблиць Microsoft Excel дозволяють швидко виконати аналітичні розрахунки. Аналізуючи результати розрахунків керівники підприємства можуть використовувати інструменти оцінки ризиків для визначення найбільш імовірних та важливих загроз, проектувати стратегії мінімізації ризиків та вдосконалення систем управління безпекою.

Крім того, для розв'язання задачі оптимізації системи інформаційної безпеки, особливо в реальних бізнес-середовищах, можна використовувати різноманітні інформаційні технології та інструменти. Наприклад, експертні системи та штучний інтелект (ШІ), аналіз даних та Великі Дані (Big Data), кіберзахист та антивірусні засоби, Системи Управління Безпекою Інформації

(СУБІ), інструменти для автоматизації процесів, блокчейн-технології, системи моніторингу та журналювання, технології контролю доступу, інструменти для оцінки ризиків.

Комбінація цих інформаційних технологій дозволяє створити комплексну систему інформаційної безпеки, яка ефективно впорається з потенційними загрозами та ризиками. Залежно від конкретних потреб та характеристик підприємства, можуть використовуватися різні комбінації технологій. Так, наприклад, використання машинного навчання для аналізу поведінки користувачів та виявлення аномалій може значно підвищити рівень виявлення загроз. Експертні системи можуть допомогти в розробці стратегій інформаційної безпеки, враховуючи великий обсяг даних та ризиків. Застосування технологій блокчейну може забезпечити безпеку та неперебільність даних, зокрема в сфері обміну конфіденційною інформацією між сторонами.

Отже, завдання інформаційної безпеки підприємства - це комплексне завдання, і успішне впровадження технологій пов'язане з необхідністю враховувати особливості конкретного підприємства, його індустрії та потенційних загроз. Крім технічних аспектів, важливо також забезпечити обізнаність персоналу, виявляти та усувати слабкі місця в безпеці, а також регулярно оновлювати та перевіряти заходи з інформаційної безпеки.

Висновки до третього розділу

1. Визначено проблеми у сфері інформаційної безпеки, а саме: зростання рівня кіберзагроз та кібератаки, недостатність відповідного фінансування для впровадження та підтримки ефективних заходів інформаційної безпеки, відсутність або застарілість технічних рішень для захисту інформації, небезпека внутрішніх загроз, таких як недобросовісні працівники, відсутність або недостатність законодавчого регулювання в галузі інформаційної безпеки, що ускладнює вживання заходів захисту,

відсутність або недостатність чітко визначених політик безпеки та стратегій в разі виникнення інцидентів безпеки.

2. Визначено напрями технічного захисту інформаційного середовища підприємства: захист автоматизованих систем від комп'ютерних вірусів і незаконної модифікації; захист від витоку через вторинні канали електромагнітного випромінювання за допомогою екранування обладнання, приміщень, використання генераторів маскувального шуму тощо; захист інформаційних ресурсів від несанкціонованого доступу та використання; захист юридичної значимості електронних документів, у разі довірчих відносин між двома суб'єктами господарювання а коли виникає необхідність передачі документів через комп'ютерні мережі – для визначення істинності адресата документ доповнюється «цифровим підписом».

3. На підставі проведених досліджень та узагальнення існуючих підходів до управління інформаційною безпекою сформовано загальний підхід до управління інформаційною безпекою, який складається із базису (серцевини) і ряду глибинних розмірів. Зауважимо, що розміри глибини представляють лише деякі розміри, зокрема: директиви, контроль, аспект управління ризиками, організаційний вимір, вимір обізнаності.

4. Зазначимо, що необхідно розробити певну систему нормативних документів, які безпосередньо будуть регулювати процес управління інформаційною безпекою підприємства: ініційована правлінням директива щодо управління інформаційною безпекою; корпоративна політика інформаційної безпеки, що випливає з директиви; набір детальних підполітик, що випливають із корпоративної політики інформаційної безпеки; набір стандартів компанії на основі корпоративної та детальної політики; набір адміністративних та операційних процедур, які знову ж таки випливають із детального набору підполітик.

5. Визначено основні складові методичного підходу до управління ризиками інформаційної безпеки: ідентифікація активів, визначення загроз, оцінка вразливостей, оцінка ризиків, моніторинг, аналіз та аудит ризиків,

визначення стратегій керування ризиками, вибір та впровадження контрольних заходів. Відповідно до визначеного методичного підходу до управління ризиками інформаційної безпеки запропоновано алгоритм взаємодії елементів процесу щодо управління ризиками інформаційної безпеки.

6. Обґрунтовано висновок про необхідність застосування економіко-математичних моделей, що дозволяє підприємствам більш раціонально розуміти витрати та ефективність заходів з інформаційної безпеки, сприяючи вирішенню важливих завдань у контексті економічної безпеки. Така модель дозволяє підприємству знайти оптимальний розподіл ресурсів між різними заходами з інформаційної безпеки, забезпечуючи заданий рівень ефективності та обмежуючи рівень ризику. Можна використовувати числові методи оптимізації, такі як методи градієнтного спуску або еволюційні алгоритми, для знаходження оптимального рішення. Цей приклад лише ілюструє загальний підхід до використання математичних моделей у сфері управління інформаційною безпекою, і конкретні функції вартості, ефективності та ризику повинні бути адаптовані до конкретних умов та конкретних потреб підприємства.

7. В результаті дослідження отримали звичайну задачу лінійного програмування, яку розв’язати з використанням сиплексного методу (що є складним при збільшенні кількості змінних), з використанням спеціалізованих надбудов електронних таблиць Microsoft Excel або з підключенням та застосуванням бібліотек для мови програмування Python, яка називається PuLP (бібліотека PuLP автоматично визначає оптимальний розподіл бюджету для мінімізації ризиків за заданих обмежень). Результати розрахунків свідчать про те, що економічний ризик на ПрАТ ДТЕК «ПАВЛОГРАДВУГІЛЛЯ» можна за відповідних заходів управління інформаційною безпекою значно знизити. Було розраховано 3 варіанти розрахунків за оптимізаційною моделлю.

ВИСНОВКИ

1. Зазначено, що інформаційну безпеку можна визначити як такий стан щодо захисту інформації від небажаного доступу, розголошення, видозміни, пошкодження або знищення тощо. Наголосимо, що у загальному формулюванні інформаційна безпека передбачає гарантування конфіденційності, цілісності та доступності інформації, яка використовується підприємством.

2. Виділено взаємозв'язок безпеки та інформаційної безпеки, який спрямований на збереження конфіденційності, цілісності та доступності інформації. На наше переконання це основоположна тріада щодо формування принципів інформаційної безпеки, яка являється запорукою надійного захисту інформації на підприємстві.

3. Встановлено, що перш ніж підприємство зможе почати розглядати будь-які ризики, пов'язані з інформацією, середовище ризиків інформаційної безпеки підприємства має бути належним чином оцінено. Діяльність з оцінки ризиків інформаційної безпеки загалом складається з трьох процесів: ідентифікація ризиків; аналіз ідентифікованих ризиків; оцінка ризиків інформаційної безпеки.

4. ПАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» є частиною вертикально інтегрованої енергетичної Групи ДТЕК і, відповідно, значна частина її продукції продається підприємствам, пов'язаним з ДТЕК. Інтегрований показник фінансового стану за досліджуваний період знаходиться в межах 8,46-8,65 і вказує на досить високий рівень фінансового стану відповідно рейтинг фінансового стану – А. Підхід Групи ДТЕК, до якої належить ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ», до ризик-менеджменту передбачає комплексну систему внутрішнього контролю та управління ризиками, засновану на стратегічному та поточному плануванні. Функція ризик-менеджменту представлена в ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» як на

рівні корпоративного центру, так і на рівні підприємств.

5. Відмітимо, що на підприємстві немає спеціалізованого відділу економічної безпеки, всі обов'язки, пов'язані з забезпеченням економічної безпеки покладені на працівників служби економіки та фінансів. Хоча економічний і фінансовий сектори відіграють важливу роль у цьому процесі, відповідальність за економічну безпеку розподілена між різними функціональними сферами та відділами. Були визначені загрози зовнішнього та внутрішнього оточення для ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ», а також визначені сильні сторони компанії.

6. Проаналізувавши складові економічної безпеки підприємства відмітимо, що інформаційна, інтелектуальна, екологічна, силова складові на високому рівну. Оцінка 0,5 (кадрова складова) свідчить про ослаблення економічної безпеки підприємства (вище ми зазначали що існують деякі проблеми із зайнятістю, через низьку заробітну платню). Загальний рівень економічної безпеки є задовільний. Можна зробити загальний висновок, що формування підходів щодо забезпечення економічної безпеки ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» є ключовим питанням сучасного стану розвитку підприємств, формування та вдосконалення систем управління.

7. Створення політики управління інформаційною безпекою є ключовим елементом забезпечення захисту інформації для ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ». В ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» розроблена політика «Управління інформаційною безпекою технологічної інфраструктури ТОВ ДТЕК ЕНЕРГО», який являється внутрішнім нормативно-правовим документом щодо формування процесу управління у сфері інформаційної безпеки. Політика визначає основні принципи, стандарти та вимоги, які спрямовані на забезпечення конфіденційності, цілісності та доступності даних та інфраструктури. Відмітимо, що управління інформаційною безпекою в ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» належить до компетенції відділу забезпечення інформаційної безпеки - це структура або команда в організації, відповідальна за забезпечення безпеки інформації

та технологій. Роль апарату директора з інформаційної безпеки включає в себе розробку та впровадження стратегій і політик інформаційної безпеки, моніторинг та виявлення потенційних загроз, а також взаємодію з іншими відділами для забезпечення відповідності та ефективності заходів з безпеки.

8. Забезпечення захисту інформації для підприємств є важливим завданням, оскільки вугільна галузь та енергетичні компанії стають об'єктами підвищеної уваги для зловмисників та кібератак. Інформаційний захист включає в себе широкий спектр заходів та стратегій для забезпечення конфіденційності, цілісності та доступності даних та інфраструктури, а саме: визначення відповідальності за використання інформаційних ресурсів; розробка, реалізація, впровадження та моніторинг виконання планів дій, щодо забезпечення інформаційної безпеки; підготовка користувачів і технічних фахівців до вирішення завдань, пов'язаних з інформаційною безпекою; проєктування та вдосконалення системи захисту інформаційної безпеки; аудит стану інформаційної безпеки підприємства.

9. Визначено проблеми у сфері інформаційної безпеки, а саме: зростання рівня кіберзагроз та кібератаки, недостатність відповідного фінансування для впровадження та підтримки ефективних заходів інформаційної безпеки, відсутність або застарілість технічних рішень для захисту інформації, небезпека внутрішніх загроз, таких як недобросовісні працівники, відсутність або недостатність законодавчого регулювання в галузі інформаційної безпеки, що ускладнює вживання заходів захисту, відсутність або недостатність чітко визначених політик безпеки та стратегій в разі виникнення інцидентів безпеки.

10. На підставі проведених досліджень та узагальнення існуючих підходів до управління інформаційною безпекою сформовано загальний підхід до управління інформаційною безпекою, який складається із базису (серцевини) і ряду глибинних розмірів. Зауважимо, що розміри глибини представляють лише деякі розміри, зокрема: директиви, контроль, аспект управління ризиками, організаційний вимір, вимір обізнаності.

11. Визначено основні складові методичного підходу до управління ризиками інформаційної безпеки: ідентифікація активів, визначення загроз, оцінка вразливостей, оцінка ризиків, моніторинг, аналіз та аудит ризиків, визначення стратегій керування ризиками, вибір та впровадження контрольних заходів. Відповідно до визначеного методичного підходу до управління ризиками інформаційної безпеки запропоновано алгоритм взаємодії елементів процесу щодо управління ризиками інформаційної безпеки.

12. Обґрунтовано висновок про необхідність застосування економіко-математичних моделей, що дозволяє підприємствам більш раціонально розуміти витрати та ефективність заходів з інформаційної безпеки, сприяючи вирішенню важливих завдань у контексті економічної безпеки. В результаті дослідження отримали звичайну задачу лінійного програмування, яку розв’язати з використанням сиплексного методу (що є складним при збільшенні кількості змінних), з використанням спеціалізованих надбудов електронних таблиць Microsoft Excel або з підключенням та застосуванням бібліотек для мови програмування Python, яка називається. Результати розрахунків свідчать про те, що економічний ризик на ПрАТ ДТЕК «ПАВЛОГРАДВУГІЛЛЯ» можна за відповідних заходів управління інформаційною безпекою значно знизити. Було розраховано 3 варіанти розрахунків за оптимізаційною моделлю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Акімова Н.С., Кирильєва Л.О., Наумова Т.А. Інформаційна безпека підприємств торгівлі в умовах становлення глобального інформаційного суспільства. *Підприємництво і торгівля*. 2023. №35. С.5-10.

2. Аніловська Г. Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. URL: http://www.nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_ 9.pdf

3. Бабенко А.О. Застосування сучасних інформаційних систем і технологій у діяльності логістичних компаній. Сучасні інформаційні технології та системи в управлінні: зб. матеріалів І Всеукр. наук.практ. конф. молодих вчених, аспірантів і студентів. 2017. С. 14-16.

4. Баланюк І.Ф., Максимюк М.М. Сутність економічної безпеки підприємства. *Інноваційна економіка*. 2016. № 1-2. С. 246-251.

5. Бессмертная Д.В. Інформаційно-аналітичні системи і технології прийняття рішень в економіці. Інформаційні технології та системи в управлінні: зб. матеріалів І Всеукр. наук.практ. конф. молодих вчених, аспірантів і студентів. 2017. С. 20-23.

6. Богуш В., Юдін О. Інформаційна безпека держави. К.: «МК-Прес», 2005. 432 с.

7. Босак А.О., Вержиковський В.П., Калінін І.Є., Максимів І.Д., Приступа Д.А., Ривак О.І. Засади формування інформаційної безпеки підприємства. *Інтернаука*. 2023. № 11. С.23-29.

8. Бурак М.В. Інформаційна безпека як складова національної безпеки України. Економічна та інформаційна безпека: проблеми та перспективи. Матеріали Всеукраїнської науково-практичної конференції. 2017. С. 21-24.

9. Васильців В.Г. Сектор інформаційних технологій та його місце та роль у системі економічної безпеки держави. Науковий вісник НЛТУ України. 2016. Вип. 26.6. С. 300-307.

10. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз’яснення Держспецзв'язку». URL: https://www.kmu.gov.ua/news/vymohy-do-zakhystu-informatsii-v-inforzviazku

11. Ворохоб М., Киричок Р., Яскевич В., Добришин, Ю., Сидоренко, С. Сучасні перспективи застосування концепції Zero Trust при побудові політики інформаційної безпеки підприємства. *Кібербезпека: освіта, наука, техніка*. 2023. №1(21). С. 223–233.

12. Волот О. Інформаційна та кібернетична безпека сучасного підприємства: забезпечення та моделювання. *Центральноукраїнський науковий вісник*. Економічні науки. 2019. Вип. 3(36). С. 238–247.

13. Гапак Н.М., Дочинець І.В.Суть та еволюція поняття «економічна безпека підприємства». *Науковий вісник Ужгородського університету*. 2014. Вип. 2(43). С. 68–73.

14. Голиков І.В. Сутність та еволюція поняття економічна безпека. *Проблеми економіки*. 2014. № 1. С. 309–314.

15. Гончаренко Є.О. Вибір підходу до оцінки ризиків інформаційної безпеки для підприємств роздрібної торгівлі. Магістерська дисертація: 125 Кібербезпека. Київ. 2019. 80 с.

16. Дейнега О.В. Інформаційна безпека підприємств в умовах глобалізації. *Економіка та суспільство*. 2019. Вип. 20. С.70-79.

17. Демчишак Н.Б., Глутковський М.О. Розвиток цифрової економіки в Україні: концептуальні основи, пріоритети та роль інновацій. *Інноваційна економіка.* 2020. №5-6. С. 43-48.

18. Зеленко О.О. Особливості розвитку інформаційних технологій в туристичній індустрії України. URL:http://nbuv.gov.uaJRN/Nvdu_2014_11_5.

19. Іжболдін М.М. Властивості інформації в системі управління інформаційною безпекою підприємства. Молодь, наука, бізнес: традиційні й нові аспекти досліджень: тези доповідей науково-практичної конференції 29.03-31.03.2023 р. : Дніпро : Друкарня «Стандарт» (ПП Бойко В.В.), 2023. С.47-49.

20. Іжболдін М.М. Засоби контролю інформаційної безпеки Облік, аудит, оподаткування та звітність у системі забезпечення економічної стійкості підприємств: тези доповідей VII Всеукраїнської науково-практичної Інтернет-конференції 11-12 травня 2023 р. Дніпро, 2023. С. 177-179.

21. Іжболдін М.М., Васільєва Л.М. Механізми та підходи щодо забезпечення інформаційної безпеки підприємницької діяльності як елемента інформаційної безпеки держави. *Публічне адміністрування і управління в Україні*. 2023. Випуск 36. С.28-32.

22. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. 2016. Вип. 2. № 1. С. 27–32.

23. Інформаційна безпека компанії та працівників – кожен має свою роль. URL: https://eba.com.ua/informatsijna-bezpeka-kompaniyi-ta-pratsivnykiv-kozhen-maye-svoyu-rol/ (дата звернення 10.10.2023).

24. Ковшик В. І. Інформаційні технології в контексті управління логістичними витратами промислових підприємств. *Вісник Хмельницького національного університе*т. Економічні науки. 2015. № 4 (1). С. 208-212.

25. Кузьомко В. Інформаційна безпека бізнесу в умовах цифрової трансформації економіки. *Зб. наук. пр. ДВНЗ «КНЕУ ім. Вадима Гетьмана».* 2021. С. 26-28.

26. Кургузенкова Л.А. Економічна безпека підприємства: сутність та чинники формування її відповідного рівня. *Економіка і суспільство*. 2015. №1. С. 31-34.

27. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства. *Економіка. Менеджмент. Бізнес*. 2015. № 3(13). С. 87–92.

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

29. Мазник Л.В., Драган О.І. Інформаційна безпека організації як фактор посилення бренду роботодавця. *Київський економічний науковий журнал*. 2023. №1. С. 39-44.

30. Марущак А. Дослідження проблем інформаційної безпеки у юридичній науці. *Правова інформатика*. 2010. № 3 (27). С. 17–21.

31. Маркіна І.А., Дячков Д.В. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва.* 2016. № 3(1). С. 80–88.

32. Нехай В.А., Нехай В.В. Інформаційна безпека як складова економічної безпеки підприємств. Науковий вісник Міжнародного гуманітарного університету. 2017. URL: http://www.vestnik-econom. mgu.od.ua/201730.pdf.

33. Ольшанська О.В. Основні положення інформаційної безпеки та її стан в сучасних умовах розвитку в Україні. Вісник Київського національного університету технологій та дизайну. 2015. № 2. С. 62-68.

34. Організаційне та методичне забезпечення виконання дипломних робіт для здобувачів вищої освіти за освітньо-професійною програмою «Управління фінансово-економічною безпекою» за спеціальністю 073 «Менеджмент» галузі знань 07 «Управління та адміністрування» другого (магістерського) рівня вищої освіти : навч. посіб. / Л. М. Васільєва, І. П. Приходько, Г. Є. Павлова, О. В. Чернецька, Т. П. Погорєлова, О. М. Губарик, С. В. Юрченко; за заг. ред. Л. М. Васільєвої, І. П. Приходька. Дніпро : Біла К. О., 2022. 183 с.

35. Павлюк Т., Волонтир Л. Використання сучасних інформаційних технологій в сільському господарстві. *Формування ринкової економіки в Україні*. 2017. № 38. С. 122-127.

36. Панченко О. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект : монографія. Київ : КВІЦ, 2020. 332 с.

37. Панченко О.А., Панченко Л.В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. *Правова*

інформатика. 2015. № 2(46). С.32-38.

38. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства. Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації. *Міжнародний збірник наукових праць*. 2014. Вип. 2. С. 165–168.

39. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства. *Науковий вісник Ужгородського національного університету*. Серія «Право». Випуск 43. Том 1. 2017. С. 34–39.

40. Правдивець О. Аналіз результатів вітчизняних наукових досліджень у напрямку інноваційного розвитку системи економічної безпеки підприємства на основі цифрових технологій. *Вчені записки Університету «КРОК»*. 2023. №1(69). С. 15–28.

41. Прозоров А.Ю. Ціннісні основи інформаційної безпеки особи, суспільства та держави. *Інформаційна безпека людини, суспільства, держави*. 2016. № 1 (20). С. 29–37.

42. Ракіпов В.Р. Стратегічне управління територіальним розвитком в умовах цифрової трансформації : автореф. дис. ... канд. екон. наук. Одеса, 2021. 21 с.

43. Ситник Г.В., Блакита Г.В., Гуляєва Н.М. Економічна безпека підприємництва в Україні. Київ : Київ. нац. торг.-екон. ун-т, 2020. 284 с.

44. Смачило Т. В., Кахній М. І. Теоретичні засади управління системою інформаційної безпеки підприємства. *Молодий вчений*. 2016. № 12.1(40). С. 969–972.

45. Сотниченко В.М. Інформаційна безпека як базова складова економічної безпеки телекомунікаційного підприємства. *Економіка. Менеджмент. Бізнес*. 2017. № 1. С. 58-66.

46. Стандарти інформаційної безпеки URL: https://www.dqsglobal.com/uk-ua/standarti-informacijnoyi-bezpe-oglyad

47. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України : дисер. док. юрид. наук: 12.00. Ужгород. 2019. 487 с.

48. Ткачук Г. О. Цифрові трансформації: взаємозв'язок із системою економічної безпеки підприємства. *Економіка харчової промисловості*. Том 11, Випуск 4/2019. С. 42-50.

49. Урсул А., Цтрдя Т. Інформаційна безпека. Сутність, зміст та принципи її забезпечення. URL: http://security.ase.md/publ/ru/pubruhtml

50. Фукс А.Е. Оцінка технологічного розвитку економіки України. М-во освіти і науки України. ДВНЗ "Київ. нац. екон. унт ім. Вадима Гетьмана". 2009. № 11. С. 32-35.

51. Черниш Р.Ф., Ігнатюк М.В. Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти. *Юридичний науковий електронний журнал*. 2022. №1. С.213-216.

52. Чубаєвський В., Жук Т. Економічна ефективність інформаційної безпеки підприємств торгівлі. *Цифрова економіка*. 2022. №1. С. 106-117.

53. Шашина М.В., Володін В.В. Інформаційна складова економічної безпеки підприємства. *Ефективна економіка*. URL: http://www.econo my.nayka.com.ua/?op=1&z=5176.

54. Яровенко Г.М. Інформаційна безпека як драйвер розвитку національної економіки : автореф. дис. ... д-ра екон. наук. Суми, 2021. 37 с.

55. Ярославський А.О., Правдюк Н. Л. Управління економічною безпекою підприємства. *Норвезький журнал розвитку міжнародної науки*. 2020. № 42 (3). С. 41–44.

56. Buck C., Olenberger C., Schweizer A., Völter F., Eymann T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*. 2021. 110.

57. Chen Y., Hu H.-c., Cheng G.-z. Design and implementation of a novel enterprise network defense system bymaneuveringmulti-dimensional network properties. *Frontiers of Information Technology & Electronic Engineering*. 2019. №20(2) P. 238–252.

ДОДАТКИ

Додаток А

Оцінка майна та капіталу ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» 2018-2022 рр., тис. грн.

Види активів (майна) та пасивів (капіталу)	2018 р.	2019 р.	2020 р.	2021 р.	2022 р.	2022 р. у % до 2018 р.
Майно - усього	24412254,0	42932637,0	38458791,0	36613431,0	41612699,0	170,46
Необоротні активи	17808341,0	26149105,0	23424206,7	28481270,0	25737679,0	144,53
Основні засоби	14266839,0	20025339,0	17938575,0	17878470,0	17008849,0	119,22
Оборотні активи	6603913,0	16783532,0	15034584,3	8132161,0	15875020,0	240,39
Запаси	699261,0	447632,0	400986,0	490154,0	535362,0	76,56
Поточна дебіторська заборгованість	5279059,0	15610825,0	13984080,6	7522073,0	15338114,0	290,55
Гроші, їх еквіваленти та поточні фінансові інвестиції	347,0	10750,0	9629,8	29994,0	12226,0	3523,34
Інші оборотні активи	545070,0	650560,0	582767,6	37525,0	74,0	0,01
Витрати майбутніх періодів	71313,0	3562,0	3190,8	46342,0	50601,0	70,96
Капітал- усього	24412254,0	42932637,0	38458791,0	36613431,0	41612699,0	170,46
Власний капітал	9401624,0	24064283,0	21556636,0	13620482,0	18124746,0	192,78
Зареєстрований (пайовий) капітал	1395431,0	1395431,0	1250018,5	1395431,0	1395431,0	100,00
Зобов'язання і забезпечення	15010633,0	18868354,0	16902155,0	22992949,0	23487953,0	156,48
Довгострокові зобов'язання	5040571,0	12014001,0	10762067,9	15826947,0	15623380,0	309,95
Поточні зобов'язання	9970062,0	6854353,0	6140087,1	7166002,0	7864573,0	78,88
Поточна кредиторська заборгованість	3713287,0	4087746,0	3661777,6	3137872,0	2335018,0	62,88

Додаток Б

Оцінка руху та функціонального стану основних засобів
ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» 2018-2022 рр., тис. грн.

№ з/п	Показник	2018 р.	2019 р.	2020 р.	2021 р.	2022 р.	Відношення у % 2022 р. до 2018 р.
Вихідна інформація, тис. грн							
1	Вартість основних засобів на п.р.	15328837,0	17916754,0	29744465,0	26644908,0	30981846	202,11
2	Надійшло за рік	302472,0	315632,0	265741,0	348080,0	82640	27,32
3	Вибуло за рік	14145,0	18175,0	33562,0	44756,0	22334	157,89
4	Вартість основних засобів на кінець року	17916754,0	29744465,0	26644908,0	30981846,0	17905168	99,94
5	Знос основних засобів: а) на початок року	1297895,00	3649915,00	9719126,00	8706333,03	13103376,00	1009,59
6	б) на кінець року	3649915,00	9719126,00	8706333,03	13103376,00	896319,00	24,56
Показники руху основних засобів							
7	Річний приріст(+) або зменшення(-), тис.грн.	2587917,00	11827711,00	-3099557,01	4336938,01	13076678,00	-505,30
8	Темп зростання (зниження), %	116,88	166,01	89,58	116,28	57,79	49,44
9	Темп приросту (зменшення), %	16,88	66,01	10,42	16,28	42,21	-250,01
10	Коефіцієнт оновлення, %	1,69	1,06	1,00	1,12	0,46	27,34
11	Коефіцієнт вибуття, %	0,09	0,10	0,11	0,17	0,07	78,12
12	Період оновлення, років	62,66	104,20	113,06	104,65	256,77	409,79
13	Коефіцієнт заміни (простого відтворення),%	4,68	5,76	12,63	12,86	27,03	577,91
14	Коефіцієнт розширення, %	855,59	3747,31	1166,38	1245,96	15823,67	1849,45
15	Період обороту, років	7,07	3,93	7,84	6,55	2,00	28,33
Показники функціонального стану основних засобів							
16	Коефіцієнт зносу, %: а) на початок року	8,47	20,37	32,68	32,68	42,29	33,83
	б) на кінець року	3,81	54,25	29,27	49,18	2,89	-0,92
17	Коефіцієнт придатності,%: а) на початок року	108,47	120,37	132,68	132,68	142,29	33,83
	б) на кінець року	123,81	154,25	129,27	149,18	102,89	-20,92

Додаток В

Фінансові результати діяльності ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ», тис. грн.

Показник	2018 р.	2019 р.	2020 р.	2021 р.	2022 р.	Відношення у % 2022 р. до 2018 р.
Чистий дохід від реалізації продукції	18105310,00	19689599,00	16379270,00	30906851,00	23901963	132,02
Операційні витрати, у тому числі: а) собівартість реалізованої продукції (товарів, робіт, послуг);	11676313,00	15837768,00	13584267,00	18529925,00	13882861	118,90
б) адміністративні витрати;	298779,00	345713,00	713491,00	773626,00	785158	262,79
в) витрати на збут;	226806,00	324002,00	350712,00	940287,00	319152	140,72
г) інші операційні витрати.	3612157,00	2266575,00	793729,00	663308,00	1632912	45,21
Валовий прибуток (збиток)	29781623,00	35527367,00	29963537,00	49436776,00	37784824	126,87
Валовий прибуток (збиток) у % до чистого доходу (виручки) від реалізації продукції (товарів, робіт, послуг)	164,49	180,44	182,94	159,95	158,08	96,10
Прибуток (збиток) від операційної діяльності	2598411,00	2186313,00	7863455	8858063,00	6713940	258,39
Фінансові та інвестиційні доходи	122266,00	58287,00	1159304,00	2099277,00	2136580	1747,48
Фінансові та інвестиційні витрати	2355657,00	1627641,00	2250057,00	3449198,00	1118544	47,48
Фінансовий результат до оподаткування	365020,00	616959,00	9646133	7508142,00	7697743	2108,86
Чистий прибуток (збиток)	647150,00	226279,00	7915406	6066763,00	6273410	969,39
Чистий прибуток (збиток) у % до чистого доходу від реалізації продукції (товарів, робіт, послуг)	1,25	3,29	48,32	19,63	26,24	2100,06
Чистий прибуток (збиток) у % до валового прибутку (збитку)	0,76	1,82	26,41	12,27	16,60	2185,20

Додаток Д

Оцінка ділової активності ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ» 2018-2022 рр.

№ з/п	Показник	2018 р.	2019 р.	2020 р.	2021 р.	2022 р.	Відношення у % (відхилення,+;-) 2022р. до 2018р.
Вихідна інформація, тис. грн.							
1	Чистий дохід від реалізації продукції	18105310,00	19689599,00	16379270,00	30906851,00	23901963,00	132,02
2	Середньорічна вартість капіталу	22666291,00	33672445,50	40695714,00	37536111,00	39113065,00	172,56
3	Середньорічна вартість необоротних активів	9269597,50	16732953,50	22810459,52	17588559,02	15872614,00	171,23
4	Середньорічна вартість оборотних активів	17008550,00	21978723,00	24786655,86	25952738,36	27109474,50	159,39
5	Середньорічна вартість оборотних виробничих фондів та готової продукції і товарів	827524,00	573446,50	424308,99	445569,99	512758,00	61,96
6	Середньорічна величина поточної дебіторської заборгованості	4476561,00	10444942,00	14797452,80	10753076,80	11430093,50	255,33
7	Середньорічна вартість власного капіталу	9269597,50	16732953,50	22810459,52	17588559,02	15872614,00	171,23
8	Середньорічна величина кредиторської заборгованості	2931486,00	3610226,00	3550004,74	3170866,24	2650153,00	90,40
Показники ділової активності							
9	Загальний коефіцієнт обертання капіталу	0,80	0,58	0,40	0,82	0,61	76,50
10	Фондовіддача необоротних активів, грн	1,95	1,18	0,72	1,76	1,51	77,10
11	Коефіцієнт обертання оборотних активів	1,06	0,90	0,66	1,19	0,88	82,83
12	Тривалість одного обороту оборотних активів, днів	338	402	545	302	408	120,73
13	Коефіцієнт обертання оборотних виробничих фондів та готової продукції і товарів	21,88	34,34	38,60	69,36	46,61	213,06
14	Тривалість одного обороту оборотних виробничих фондів, днів	16	10	9	5	8	46,94
15	Коефіцієнт обертання поточної дебіторської заборгованості	4,04	1,89	1,11	2,87	2,09	51,70
16	Тривалість одного обороту поточної дебіторської заборгованості, днів	89	191	325	125	172	193,41
17	Коефіцієнт обертання власного капіталу	1,95	1,18	0,72	1,76	1,51	77,10
18	Тривалість одного обороту власного капіталу,днів	184	306	501	205	239	129,71

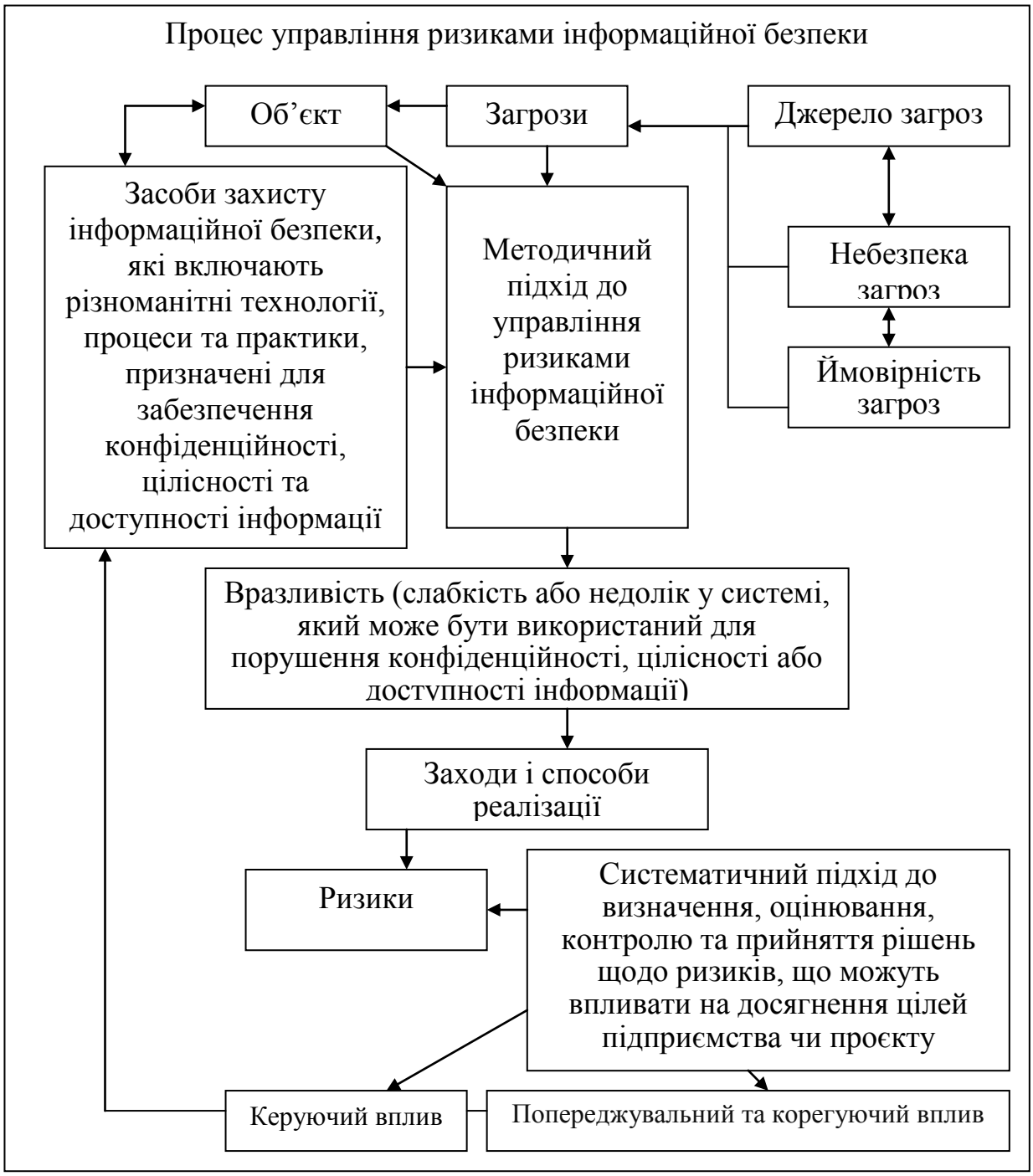
Додаток Е

Комплексна (рейтингова) оцінка фінансового стану ПрАТ «ДТЕК ПАВОГРАДВУГІЛЛЯ»

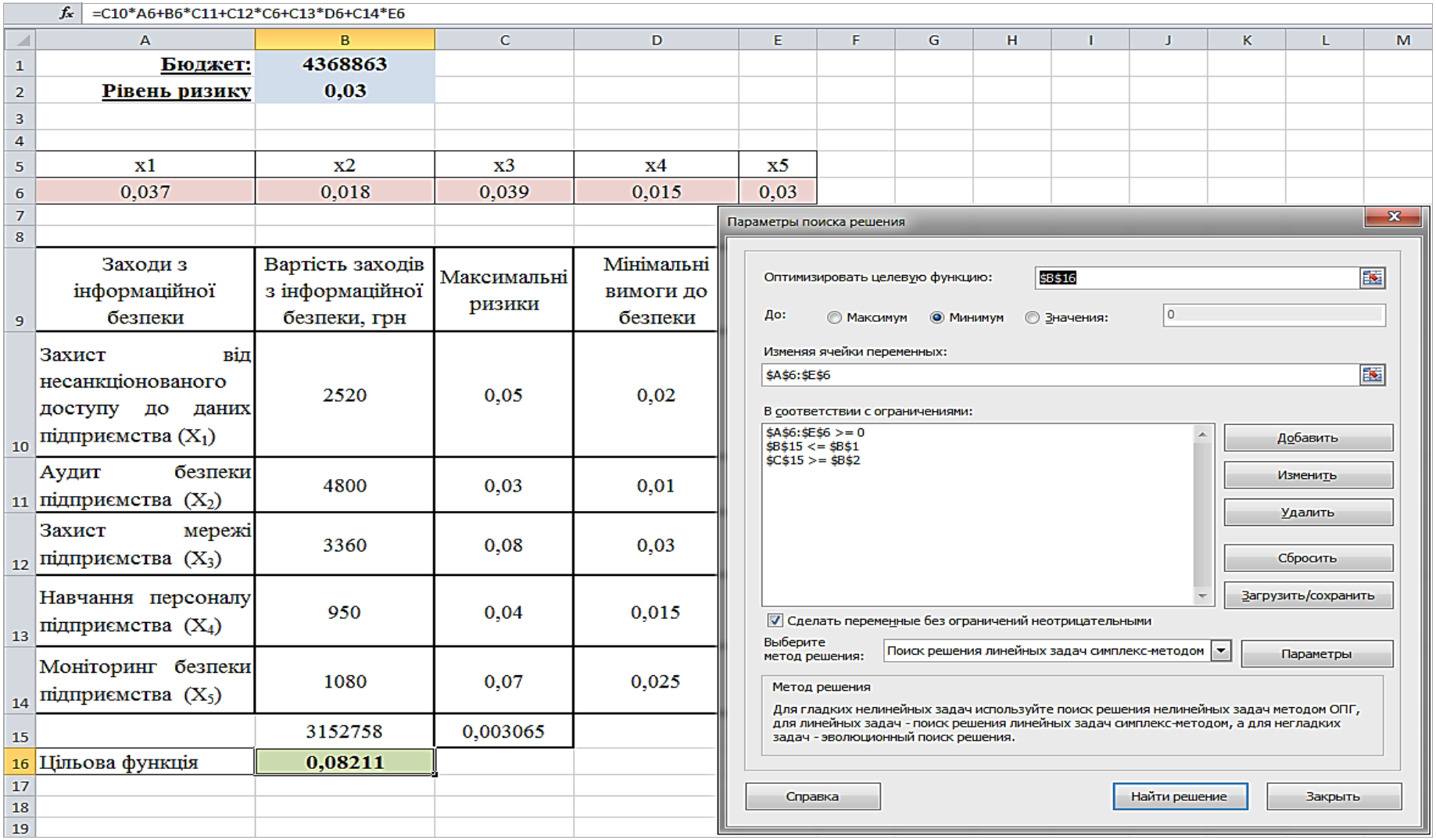
№ з/п	Показники	2018 р.		2019 р.		2020 р.		2021 р.		2022 р.		Питома вага (Vi, %) в інтегрованому показнику
		Значення	Рейтинг	Значення	Рейтинг	Значення	Рейтинг	Значення	Рейтинг	Значення	Рейтинг	
1	***Показники ліквідності***											
1.1	Коефіцієнт поточної ліквідності (загальний коефіцієнт покриття)	0,66	10	2,45	10	2,45	10	1,13	10	2,02	10	8
1.2	Коефіцієнт швидкої ліквідності	0,53	10	2,28	9	2,28	10	1,05	10	1,95	5	8
2	***Показники ділової активності***											
2.1	Період оборотності дебіторської заборгованості, днів	89,01	8	190,97	10	325,23	10	125,25	9	193,41	10	9
2.2	Період оборотності оборотних виробничих фондів та готової продукції і товарів, днів	12,20	3	4,81	3	3,97	2	4,38	4	5,61	1	9
2.3	Період оборотності активів, днів	184,31	9	305,94	10	501,35	10	204,87	10	129,71	10	9
3	***Показники фінансової незалежності***											
3.1	Коефіцієнт фінансової незалежності, %	61,49	10	43,95	10	43,95	10	62,80	10	48,69	10	9
3.2	Частка оборотних активів, сформованих за рахунок власних коштів, % (коефіцієнт забезпеченості оборотних коштів)	-50,97	10	59,16	10	59,16	10	11,88	10	41,02	10	9
4	***Показники рентабельності***											
4.1	Рентабельність продажу, %	2,02	10	3,13	10	24,29	10	24,29	9	21,54	8	9
4.2	Рентабельність активів, % (загальна рентабельність (збитковість) капіталу)	1,61	10	1,83	10	20,00	10	20,00	10	12,22	10	9
4.3	Рентабельність капіталу, % (загальна рентабельність (збитковість) власного капіталу)	2,44	10	3,69	10	42,69	10	42,69	9	12,32	8	9
5	***Інші показники***											
5.1	Коефіцієнт зносу основних засобів	20,37	8,00	32,68	8	32,68	7	42,29	8	24,57	6	7
5.2	Частка простроченої кредиторської заборгованості, %	151,74		43,01		43,01		17,56		29,41		5
	Інтегрований показник фінансового стану	**8,46**		**8,65**		**8,57**		**8,55**		**8,61**		**100**
	Рейтинг фінансового стану	**A**		**A**		**A**		**A**		**A**		**-**

Додаток Ж

Алгоритм взаємодії елементів процесу щодо управління ризиками інформаційної безпеки



Приклад одного з рішень з використанням засобу «Пошук рішення» в електронних таблицях Microsoft Excel



=C10*A6+B6*C11+C12*C6+C13*D6+C14*E6

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	**Бюджет:**	4368863											
2	**Рівень ризику**	0,03											
3													
4													
5	x1	x2	x3	x4	x5								
6	0,037	0,018	0,039	0,015	0,03								
7													
8													
9	Заходи з інформаційної безпеки	Вартість заходів з інформаційної безпеки, грн	Максимальні ризики	Мінімальні вимоги до безпеки									
10	Захист від несанкціонованого доступу до даних підприємства (X_1)	2520	0,05	0,02									
11	Аудит безпеки підприємства (X_2)	4800	0,03	0,01									
12	Захист мережі підприємства (X_3)	3360	0,08	0,03									
13	Навчання персоналу підприємства (X_4)	950	0,04	0,015									
14	Моніторинг безпеки підприємства (X_5)	1080	0,07	0,025									
15		3152758	0,003065										
16	Цільова функція	**0,08211**											
17													
18													
19													

Додаток 3