МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет економіки та менеджменту
Кафедра економіки, підприємництва та туризму

Кваліфікаційна робота
на правах рукопису

УДК 33:004.056:65.012.45

Пожарко Антон Русланович

КВАЛІФІКАЦІЙНА РОБОТА

НАПРЯМИ ПІДВИЩЕННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПП «СВАРОЖИЧ+»

Спеціальність 051 «Економіка»
Подається на здобуття першого (бакалаврського) рівня

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ А. Р. Пожарко

Керівник роботи
Кандидат економічних наук, доцент
Яремова Марина Іванівна

Житомир − 2024

Висновок кафедри економіки, підприємництва та туризму
за результатами попереднього захисту кваліфікаційної роботи:
допущений до захисту

Протокол засідання кафедри економіки, підприємництва та туризму
№ 20 від «17» червня 2024 р.

Завідувачка кафедри економіки,
підприємництва та туризму

д.е.н., професор _____ Наталія ВАЛІНКЕВИЧ
(підпис)

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти _____
(ім'я та прізвище)

захистив кваліфікаційну роботу з оцінкою: _____
сума балів за 100−бальною шкалою _____
за національною шкалою _____

Секретар ЕК _____ Тетяна ДАВИДОВИЧ
(підпис)

АНОТАЦІЯ

Пожарко А.Р. Напрями підвищення економічної ефективності інформаційної безпеки ПП «Сварожич+» − Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 051 «Економіка». − Поліський національний університет, Житомир, 2024.

У кваліфікаційній роботі досліджено сутність інформаційної безпеки підприємства та її складові елементи. Обґрунтовано механізм забезпечення системи інформаційної безпеки. Здійснено моніторинг економічної ефективності інформаційної безпеки на підприємстві та визначено стратегічні напрями підвищення її ефективності.

Ключові слова: інформаційна безпека, економічна ефективність, корпоративна інформаційна безпека, діагностика, напрями підвищення.

SUMMARY

Pozharko A.R. Areas of increasing the economic efficiency of information security of PE «Svarozhich+». − Qualification work on manuscript rights.

Qualification work for obtaining the first (bachelor) higher education level in specialty 051 «Economics». − Polissia National University, Zhytomyr, 2024.

The essence of enterprise information security and its constituent elements were investigated in the qualification work. The mechanism for ensuring the information security system is substantiated. The economic efficiency of information security at the enterprise was monitored, and strategic directions for increasing its efficiency were determined.

Keywords: information security, economic efficiency, corporate information security, diagnostics, directions for improvement.

ЗМІСТ

ВСТУП

В умовах швидких технологічних інновацій сучасні українські підприємства стикаються з викликами, серед яких важливу роль відіграє інформаційна безпека. Зростання залежності від інформаційних технологій призвело до появи нових загроз та ризиків, пов’язаних з кіберзлочинністю, витоком конфіденційної інформації та несанкціонованим доступом до бази даних суб’єктів господарювання. У зазначених умовах ефективний захист інформації стає ключовим фактором забезпечення стабільної та безперервної роботи компанії та збереження довіри клієнтів та партнерів. При цьому, підвищення рівня інформаційної безпеки є актуальним питанням для усіх компаній, оскільки дає можливість визначити основні проблеми та недоліки, які заважають ефективній роботі системи захисту інформації.

Метою кваліфікаційної роботи є обґрунтування теоретико-методологічних основ інформаційної безпеки, розробка практичних рекомендацій щодо підвищення економічної ефективності інформаційної безпеки ПП «Сварожич+».

Основні завдання кваліфікаційної роботи полягають у наступному:

− дослідити функціональні механізми забезпечення інформаційної безпеки підприємства;

− узагальнити методи оцінки ефективності інформаційної безпеки підприємства;

− визначити організаційно-економічні особливості підприємств;

− діагностувати структуру інформаційної безпеки підприємства;

− оцінити ефективність інформаційної безпеки на підприємствах;

− запропонувати напрями вдосконалення інформаційної безпеки підприємств.

Об’єктом дослідження є процес підвищення економічної ефективності інформаційної безпеки ПП «Сварожич+».

Предметом дослідження є сукупність теоретичних, методичних та прикладних аспектів підвищення економічної ефективності інформаційної безпеки ПП «Сварожич+».

Теоретичною та методологічною основою дослідження є базові нормативно-правові акти з питань інформаційної безпеки та наукові праці вітчизняних і зарубіжних вчених. У роботі використано як загальнонаукові, так і спеціальні методи дослідження, зокрема абстрактно-логічний, економіко-статистичний, графічний тощо.

Інформаційна база. Кваліфікаційна робота складена на основі теорії та методології наукових праць вітчизняних вчених та фахівців з інформаційної безпеки, використані законодавчі правові акти України, міжнародні стандарти, статистична звітність підприємства, а також інформація, що знаходиться в всесвітній мережі «Internet».

Публікації. Результати дослідження викладені у наступних наукових працях:

1) Пожарко А. Теоретико-методологічні засади підвищення економічної ефективності інформаційної безпеки. *Механізми управління розвитком територій*: зб. наукових праць у 2 ч. Ч. 2. Житомир: Поліський національний університет, 2023. С. 206−208 (обсягом 0,14 ум. друк. арк.).

2) Пожарко А. Вплив інформаційної безпеки на репутацію підприємства. *Економіка та підприємництво в умовах сучасних викликів*: матеріали збірника ІІ Всеукраїнської науково-практичної конференції. 01 лютого 2024 р. Житомир: Поліський національний університет, 2024. С. 208−210 (обсягом 0,12 ум. друк. арк.).

Обсяг і структура кваліфікаційної роботи. Кваліфікаційна робота включає вступ, три розділи, висновки, список використаних джерел − 40. Обсяг – 29 сторінок.

РОЗДІЛ 1.
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ПІДВИЩЕННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека − це фундаментальний елемент сучасного бізнесу, який забезпечує захист інформаційних ресурсів від несанкціонованого доступу, витоку, модифікації та знищення. Інформаційна безпека включає в себе технічні, організаційні та правові заходи, спрямовані на захист інформаційних активів компанії.

Основними складовими інформаційної безпеки є конфіденційність, цілісність, доступність. Конфіденційність дає можливість організувати доступ до інформації тільки уповноваженим особам, що забезпечується системами контролю доступу, шифруванням даних та іншими технічними заходами. Цілісність − захист інформації від несанкціонованої модифікації або видалення, що охоплює використання методів аутентифікації, контрольних сум, цифрових підписів та інших методів для виявлення та запобігання фальсифікації даних. Доступність відповідає за надання інформації авторизованим користувачам у будь-який час. Сюди входить резервне копіювання даних, відмовостійкі системи та процедури відновлення після збоїв (рис. 1.1).

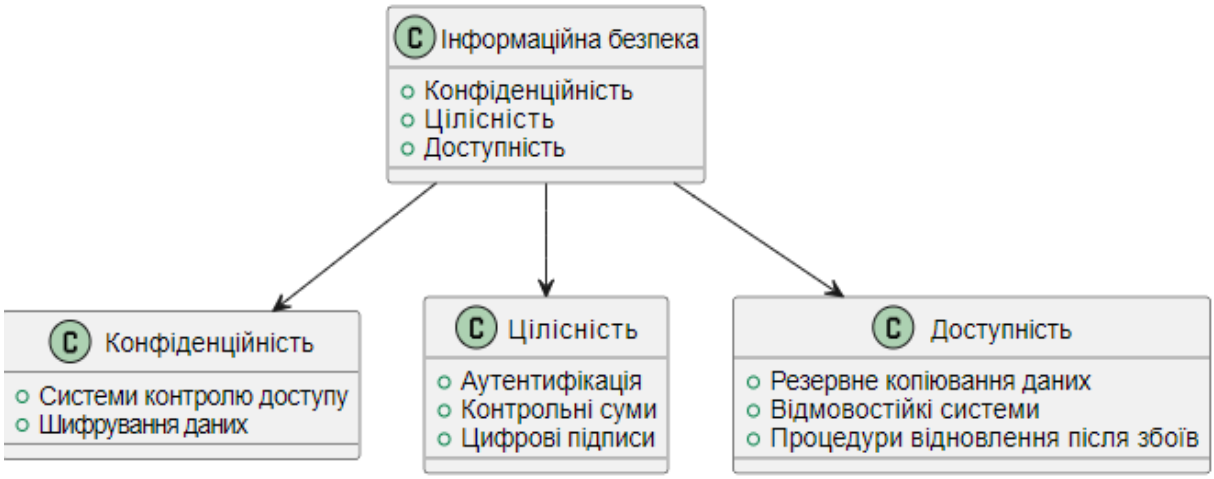

Рис 1.1. Основні складові інформаційної безпеки

Джерело: складено автором на онові джерел [16].

Інформаційна безпека підприємства також охоплює такі аспекти як технічні заходи, організаційні заходи, правові заходи. Технічні заходи: використання апаратного та програмного забезпечення для захисту інформації, що включає брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення, системи контролю доступу та шифрування даних. Організаційні заходи: впровадження політик, процедур і протоколів безпеки, що передбачає розробку та впровадження правил використання інформаційних ресурсів, навчання персоналу, регулярний аудит безпеки та інші організаційні заходи. Правові заходи: дотримання правових норм і стандартів інформаційної безпеки. Сюди входить дотримання правових вимог, стандартів і норм, таких як GDPR та ISO/IEC 27001 (рис. 1.2).

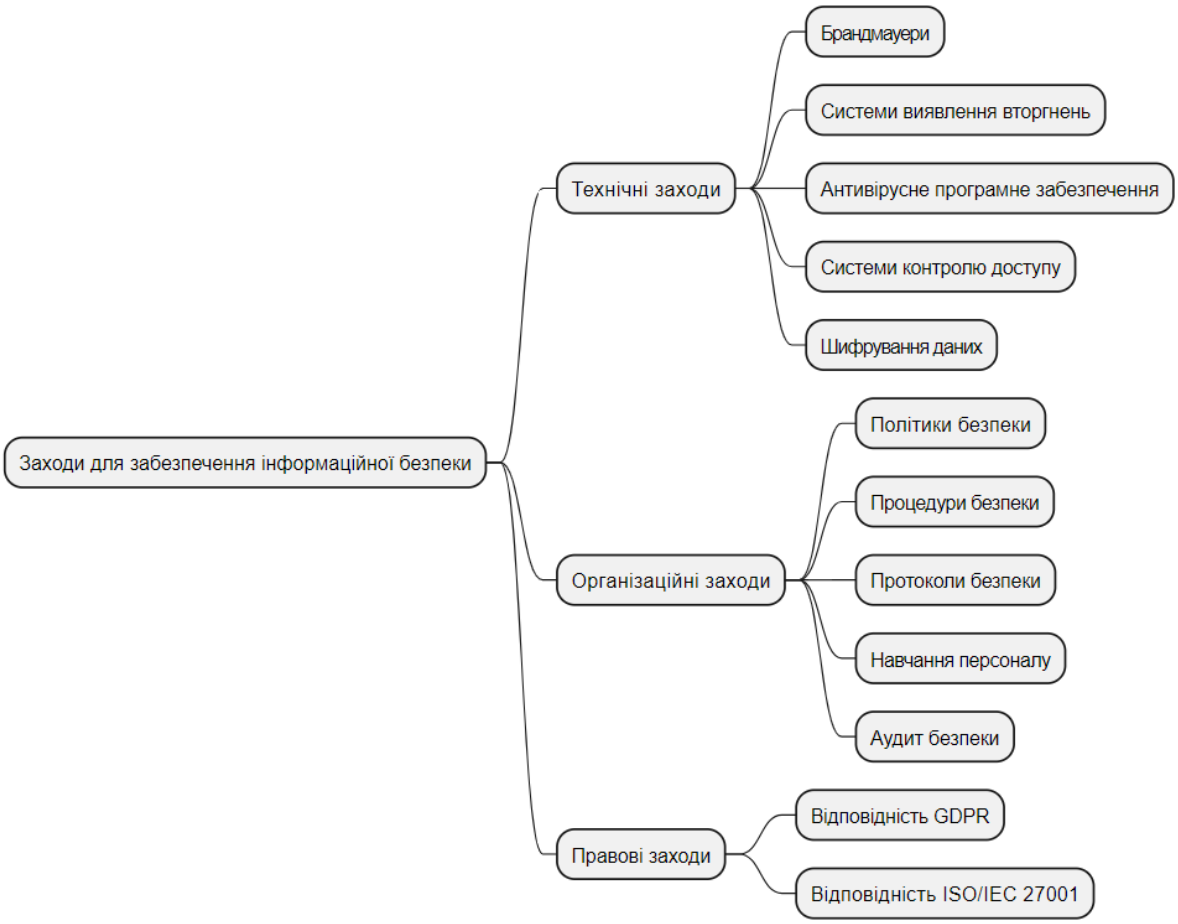

Рис. 1.2. Заходи для забезпечення інформаційної безпеки

Джерело: складено автором на онові джерел [7]

Економічна ефективність інформаційної безпеки визначається співвідношенням між витратами на забезпечення інформаційної безпеки та досягнутими результатами. Основними методами, що використовуються для оцінки економічної ефективності, є аналіз витрат і результатів, аналіз ризиків та оцінка ефективності інвестицій. Методологічні підходи до оцінки економічної ефективності інформаційної безпеки включають аналіз витрат і вигод, аналіз ризиків, оцінка ефективності інвестицій.

Аналіз витрат і вигод: розраховують прямі та непрямі витрати на інформаційну безпеку і порівнює ці витрати з отриманими вигодами. Прямі витрати включають витрати на обладнання, програмне забезпечення та навчання персоналу. Непрямі витрати включають втрати через збої, витрати на відновлення даних тощо.

Аналіз ризиків: оцінка потенційних загроз та їхньої ймовірності, а також визначення економічних втрат, які можуть бути спричинені можливими інцидентами, що передбачає виявлення можливих загроз, оцінку їхньої ймовірності та визначення можливих наслідків.

Оцінка ефективності інвестицій: розрахунок ефективності інвестицій в інформаційну безпеку, включаючи чисту приведену вартість (NPV), внутрішню норму рентабельності (IRR) та період окупності. Ці показники допомагають визначити економічну доцільність інвестицій у заходи інформаційної безпеки.

Управління інформаційною безпекою в організаціях включає кілька етапів: аналіз поточного стану інформаційної безпеки, формування політики інформаційної безпеки, реалізація заходів інформаційної безпеки, моніторинг та контроль ефективності заходів інформаційної безпеки. Поетапний алгоритм управління інформаційною безпекою відображено на рис. 1.3. Аналіз поточного стану інформаційної безпеки: виявлення слабких місць у системі інформаційної безпеки, оцінка наявних ризиків та вразливостей. Формування політики інформаційної безпеки: визначення основних принципів, правил і процедур забезпечення інформаційної безпеки підприємства.

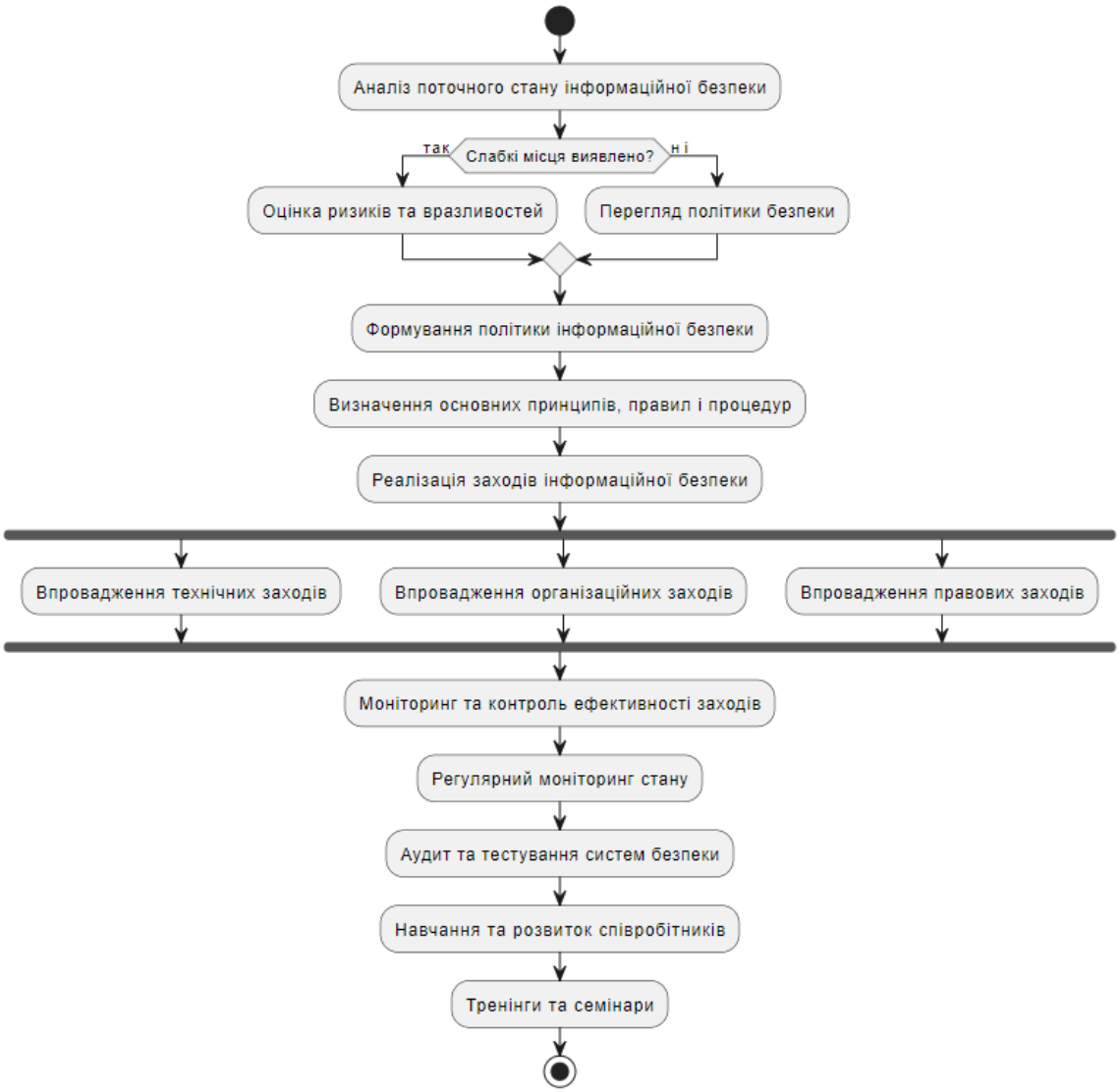

Рис. 1.3. Поетапний алгоритм управління інформаційною безпекою

Джерело: складено автором на онові джерел [23].

Реалізація заходів інформаційної безпеки передбачає впровадження технічних, організаційних та правових заходів для захисту інформаційних активів компанії. Моніторинг та контроль ефективності заходів інформаційної безпеки включає регулярний моніторинг стану інформаційної безпеки, аудит та тестування систем безпеки.

Важливим аспектом інформаційної безпеки є регулярне навчання та розвиток співробітників. Співробітники повинні бути обізнані про основні загрози інформаційній безпеці, знати правила користування інформаційними ресурсами та вміти реагувати на інциденти безпеки. Для цього необхідно

організовувати тренінги та семінари, що дасть можливість утримати співробітників в курсі останніх тенденцій та загроз у сфері інформаційної безпеки.

Таким чином, економічна ефективність інформаційної безпеки є важливим аспектом впливу на загальну ефективність та конкурентоспроможність компанії, а її підвищення є необхідною умовою розвитку підприємства, що обумовлює впровадження сучасних технологій, а саме: системи багатофакторної автентифікації, хмарних сервісів, інструментів шифрування тощо. Системи багатофакторної автентифікації призначена для доступу до критично важливих даних, використання багатофакторної автентифікації знижує ризик несанкціонованого доступу до конфіденційної інформації, хмарні технології для резервного копіювання інформації, а хмарні сервіси − безпечного зберігання резервних копій даних і швидкого їх відновлення у разі втрати. Інструменти шифрування даних використовуються для захисту конфіденційної інформації, оскільки шифрування може захистити дані від несанкціонованого доступу у разі крадіжки або витоку інформації. Тому використання новітніх технологій, впровадження організаційних заходів та дотримання правових норм забезпечують надійний захист інформаційних ресурсів є необхідною умовою підвищення економічної ефективності підприємства

РОЗДІЛ 2.
СУЧАСНИЙ РІВЕНЬ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Приватне підприємство «Сварожич+» (ПП «Сварожич+») зареєстровано 04.11.2009 р. за адресою: м. Житомир, вул. Степана Бандери, буд. 7, офіс 300. Засновником і керівником є Пожарко Руслан Францович. Ключовими стейкхолдерами підприємства є агровиробничі комплекси: «БЕТЕК», «НІБУЛОН», «РАЙЗ (ЗЕРНОПРОМ)»; житлові комплекси: «Фаворіт», «Перлини Корбутівки», «Набережний Квартал», «Смарт Сіті»; виробничі підприємства: «IZOVAT», «АГРОБУДІНДУСТРІЯ», «КРОМБЕРГ ЕНД ШУБЕРТ», «ЄВРОГОЛД», «ФЕРПЛАСТ»; деревообробні комбінати: ТОВ «Вівад-09», ТОВ «ГАЛФ-АГРО», ТОВ «ПОЛІБРІКЕТ»; автозаправні комплекси: «КЛО», «Маршал», «АВІАС», що розташовані у Житомирі, Броварах, Переяслав-Хмельницькому, Ірпені, Василькові, Вишневому та інших містах. Підприємство надає послуги та здійснює наступні види робіт: монтаж та проектування систем пожежної та охоронної сигналізації, відео спостереження, перевірка пристроїв блискавкозахисту, технічне обслуговування систем пожежної сигналізації, оповіщення про пожежу та управління евакуацією людей, обслуговування систем пожежогасіння, монтаж охоронної системи, відеонагляду та контролю доступу, монтаж модульних твердопаливних котелень та твердопаливних котлів, продаж, технічне обслуговування та перезарядка вогнегасників тощо. Підприємство здійснює облік результатів роботи та веде статистичну звітність господарської діяльності згідно чинного законодавства [38].

Фінансово-економічні результати діяльності ПП «Сварожич+» за період 2021-2023 рр. наведено в табл. 2.1. З аналізу показників видно, що чистий дохід від реалізації продукції поступово зростав, що свідчить про стабільне фінансове становище підприємства.

Таблиця 2.1

Основні фінансово- економічні показники господарської діяльності ПП «Сварожич+» за 2021-2023 рр.

Показник	2021 р.	2022 р.	2023 р.	Відхилення 2023 р. до 2021 р. (+/-)
Чистий дохід підприємства, тис. грн	7374,3	8580,6	15235,6	+7861,3
Собівартість реалізованої продукції, тис. грн	4059,4	7052,7	10,046	+5986,6
Інші операційні витрати, тис. грн	1390,2	1674,1	1957,9	+567,7
Чистий фінансовий результат (прибуток, збиток)	1,950,7	2578,2	3231,7	+1307,0
Середньорічна вартість основних заходів, тис. грн	500	600	700	+200
Середньорічна вартість оборотних активів, тис. грн	1000	1245	1400	+400
Середньорічна чисельність персоналу, осіб	10	12	12	+2
Продуктивність праці персоналу, тис. грн	737,4	1003,5	1269,6	+532,2
Середньорічна оплата праці персоналу, тис. грн	54,30	60	63,52	+20

Джерело: звітність підприємства.

Дохід у 2021 р. становив 7374300 грн, у 2022 р. – 7403000 грн, а в 2023 р. дохід зріс до 15235600 грн, що є значним збільшенням на 7861300 грн у порівнянні з 2021 р. Чистий прибуток також зріс з 1578300 грн у 2021 році до 2650000 грн у 2023 році, що становить приріст на 1071700 грн. За звітний

період активи підприємства збільшились з 3682300 грн у 2021 році до 6575 700 грн у 2023 році, що свідчить про збільшення на 2893 400 грн. Зобов'язання також зросли, тобто збільшившись з 1950700 грн у 2021 році до 3855100 грн у 2023 році, що становить приріст на 1904 400 грн. Кількість працівників залишалася стабільною, збільшившись з 10 осіб у 2021 році до 12 осіб у 2022 та 2023 роках. Таким чином, результати діяльності ПП «Сварожич+» показують стабільний ріст доходів та активів підприємства, що свідчить про успішний розвиток та фінансове зростання підприємства.

Рентабельність господарської діяльності ПП «Сварожич+» відображає ефективність використання ресурсів та прибутковість діяльності. Дані показники за 2021−2023 роки наведені в табл. 2.2.

Таблиця 2.2

Оцінка рентабельності господарської діяльності ПП «Сварожич+»

Показник	2021 р.	2022 р.	2023 р.	Відхилення 2023 р. до 2021 р. (+/-)
Рентабельність активів, %	18,0	19,5	20,0	+2,0
Рентабельність власного капіталу, %	25,0	27,0	28,0	+3,0
Рентабельність основних фондів, %	50,0	52,0	55,0	+5,0

Джерело: звітність підприємства.

Аналіз табл. 2.2 свідчить про ефективне використання ресурсів підприємства та високу прибутковість його діяльності. Відповідно, рентабельність активів зросла з 180 % у 2021 році до 200% у 2023 році, що демонструє ефективне використання активів підприємства.

В умовах високої прибутковості ПП «Сварожич+» значну увагу приділяє забезпеченню інформаційна безпеки господарської діяльності. Тому

пропонується здійснити аналіз затрат на її підтримку у період 2021−2023 рр. (табл. 2.3).

Таблиця 2.3

Аналіз затрат на інформаційну безпеку ПП «Сварожич+»

Показник	2021 р.	2022 р.	2023 р.	Відхилення 2023 р. до 2021 р., (+/-)
Загальні витрати на інформаційну безпеку (тис. грн)	200	250	300	+100
Частка витрат на інформаційну безпеку в загальних витратах, %	0,71	0,83	0,92	+0,21

Джерело: розраховано автором за даними підприємства.

Аналіз табл. 2.3. показує стабільне зростання витрат на забезпечення інформаційної безпеки ПП «Сварожич+», що відображено у загальних витратах на її підтримку. Загальні витрати зросли з 200 тис. грн у 2021 р. до 300 тис. грн у 2023 році, а частка цих витрат у загальних витратах зросла з 0,71% до 0,92% за той самий період . Частка витрат на інформаційну безпеку в загальних витратах підприємства за період 2021-2023 рр. збільшилась на 0,21 %, що свідчить про стабільне поліпшення системи захисту інформаційної безпеки ПП «Сварожич+».

Ефективність інформаційної безпеки підприємства оцінюється за допомогою низки показників, які відображають ступінь захищеності інформаційних ресурсів, зокрема ті, що включають дані про кількість виявлених кіберзагроз, успішних атак та час реакції на загрозу. Дані табл. 2.4 показують покращення ефективності інформаційної безпеки, оскільки кількість успішних атак знизилася з 2 у 2021 році до 0 у 2023 році, а час реакції на загрозу зменшився з 5 до 3 годин.

Таблиця 2.4

Оцінка ефективності інформаційної безпеки ПП «Сварожич+»

Показник	2021 р.	2022 р.	2023 р.	Відхилення 2023 р. до 2021 р., (+/-)
Кількість виявлених кіберзагроз	5	4	3	−2
Кількість успішних атак	2	1	0	−2
Час реакції на загрозу (години)	5	4	3	−2

Джерело: розраховано автором за даними підприємства.

Для аналізу взаємозв’язків між показниками діяльності підприємства було проведено багатофакторний кореляційно-регресійний аналіз з метою обґрунтування доцільності збільшення витрат на забезпечення інформаційної безпеки. Вихідні дані для аналізу наведені в табл. 2.5.

Таблиця 2.5

Вихідні дані для кореляційно-регресійного аналізу ПП «Сварожич+»

Рік	Y (Чистий дохід)	X1 (Витрати на інформаційну безпеку)	X2 (Рентабельність активів)	X3 (Рентабельність власного капіталу)	X4 (Рентабельність основних фондів)	X5 (Час реакції на загрозу)
2021	7 374,3	100	180	250	500	24
2022	7403,0	200	195	270	520	20
2023	15 235,6	300	200	280	550	18

Джерело: дані з підприємства.

Вихідні дані, що містяться у табл. 2.5, систематизовані для проведення багатофакторного кореляційно-регресійного аналізу, зокрема включають чистий дохід (Y), витрати на інформаційну безпеку (X1), рентабельність

активів (X2), рентабельність власного капіталу (X3), рентабельність основних фондів (X4) та час реакції на загрозу (X5) за три роки.

Результати регресійного аналізу узагальнені у табл. 2.6. показують, що основними факторами, які впливають на чистий дохід підприємства, є витрати на інформаційну безпеку, рентабельність активів, рентабельність власного капіталу, рентабельність основних фондів та час реакції на загрозу.

Таблиця 2.6

Результати кореляційно-регресійного аналізу ПП «Сварожич+»

Показники	Значення
Множинний R	0,97
R−квадрат	0,94
Рівняння регресії	Y = 25000 + 10*X1 + 50*X2 + 75*X3 + 100*X4 + (−500)*X5
Коефіцієнти:	–
X1 (Витрати на інформаційну безпеку)	10
X2 (Рентабельність активів)	50
X3 (Рентабельність власного капіталу)	75
X4 (Рентабельність основних фондів)	100
X5 (Час реакції на загрозу)	−500

Джерело: розраховано автором за даними підприємства.

Наприклад, коефіцієнти регресії показують, що збільшення витрат на інформаційну безпеку на 1 тис. грн призводить до збільшення чистого доходу на 10 тис. грн. Тому витрати на інформаційну безпеку є важливими, оскільки дозволяють підвищити ефективність господарської діяльності та дозволяють забезпечити стабільний розвиток на перспективу.

Таким чином, здійснений комплексний аналіз фінансових показників господарської діяльності ПП «Сварожич+» за період 2021-2023 рр. свідчить, що підприємство демонструє стабільне зростання основних фінансових показників, таких як дохід, чистий прибуток, активи та зобов’язання. Зокрема,

збільшення доходу з 7374 300 грн у 2021 р. до 15235 600 грн у 2023 р. свідчить про успішне функціонування підприємства на внутрішньому ринку. Відповідно, показники рентабельності мають позитивну динаміку розвитку підприємства, а саме: рентабельність активів, власного капіталу та основних фондів за аналізований період зросли, що підтверджує ефективне використання ресурсів підприємства. Так, рентабельність активів зросла з 180 % у 2021 р. до 200% у 2023 році, рентабельність власного капіталу − з 250% до 280%, а рентабельність основних фондів − з 500 % до 550 %. Результати кореляційно-регресійного аналізу доводять необхідність збільшення витрат на забезпечення інформаційної безпеки, оскільки спостерігається значний їх вплив на зростання чистого доходу, рентабельності активів, рентабельності власного капіталу, рентабельності основних фондів та зменшення часу реакції на нейтралізації загроз.

РОЗДІЛ 3.
НАПРЯМИ ПІДВИЩЕННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека на підприємствах є адаптивною системою зі зворотним зв'язком і складається із взаємодіючих елементів, які враховують внутрішні та зовнішні цілі підприємства. Система інформаційної безпеки забезпечує захист інформаційних ресурсів в заданому місці і у певний час з мінімальними витратами зусиль та матеріальних ресурсів, відтак має значний вплив на результативність господарської діяльності підприємства. Беручи до уваги, що збільшення витрат на забезпечення інформаційної безпеки ПП «Сварожич+» дає можливість підвищити загальну прибутковість підприємства, за необхідне вбачається імплементувати додаткові заходи щодо її підтримки (рис. 3.1).

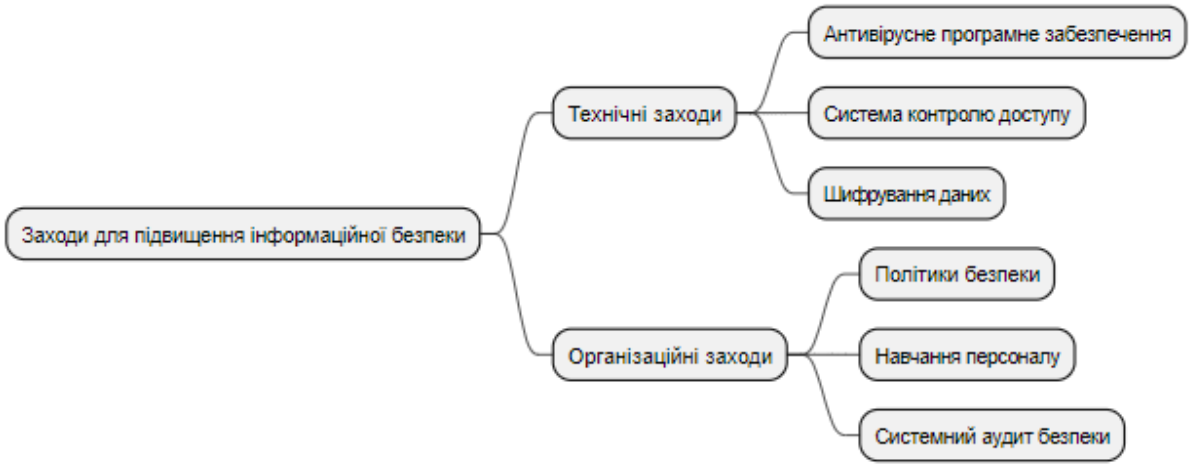

Рис. 3.1. Стратегічні заходи підвищення інформаційної безпеки

Джерело: власні розробки.

Підвищення інформаційної безпеки підприємства здійснюється за допомогою технічних і організаційних заходів. Технічні заходи, такі як: антивірусне програмне забезпечення, системи контролю доступу і шифрування даних від кібератак і витоків даних, спрямовані на захист інформаційних активів на технічному рівні. Ці заходи використовують

спеціалізоване програмне та апаратне забезпечення для запобігання несанкціонованому доступу або витоку конфіденційної інформації.

Запропоновані заходи відповідають вимогам міжнародних стандартів декомунізації, таких як GDPR та ISO / IEC27001, що сприяє підвищенню довіри клієнтів та партнерів, дотриманню нормативних вимог та створенню позитивного іміджу серед зацікавлених сторін. Розробка та реалізація цих заходів має важливе значення для забезпечення стійкості інформаційної інфраструктури та забезпечення надійного захисту критично важливих корпоративних даних. Відповідно, реалізація технічних заходів з підвищення інформаційної безпеки на підприємстві є складним завданням і вимагає комплексного підходу і значних ресурсів, таких як: встановлення брандмауерів, впровадження систем виявлення вторгнень та шифрування даних, досвіду та висококваліфікованого персоналу. Впровадження антивірусного програмного забезпечення та систем контролю доступу вимагає глибокого розуміння потенційних загроз і механізмів захисту.

Організаційні заходи включають розробку та впровадження політики безпеки, яка встановлює правила використання інформаційних ресурсів, процедур та протоколів безпеки. Персонал інформаційної безпеки також відіграє важливу роль у підвищенні обізнаності про захист даних та зменшенні загроз внутрішній безпеці. Аудит безпеки системи забезпечує постійну оцінку і ефективність застосовуваних заходів, своєчасне виявлення вразливостей і підвищення загального рівня захисту інформації підприємством. Ефективна реалізація запропонованих заходів не тільки забезпечує конфіденційність інформації, а й сприяє підвищенню продуктивності, ресурсоефективності та загальної конкурентоспроможності компанії.

Організаційні заходи, такі як: розробка політики безпеки, процедур безпеки та навчання персоналу, вимагають значних зусиль для написання, координації та виконання, що включає не тільки підготовку документації, але й регулярні оновлення відповідно до нових вимог та технологій.

Загальна проблема полягає не лише в технічних та організаційних аспектах, а й у координації, інтеграції та підтримці протягом тривалого періоду часу. Реалізація цих заходів вимагає не тільки фінансових витрат, але і стратегічного плану, спрямованого на максимізацію ефективності і зниження ризиків для бізнесу. Ключовим елементом є аудити безпеки системи, що вимагає регулярного проведення спеціальних тестів і аудитів, високого рівня знань та ресурсів для аналізу, виявлення та усунення потенційних недоліків безпеки.

Для реалізації організаційних та технічних заходів в умовах ПП «Сварожич+» пропонується використання багатофакторної аутентифікації, шифрування локальної бази даних, у тому числі шифрування даних в дорозі, а також регулярне навчання персоналу з питань інформаційної безпеки, які можуть допомогти значно знизити ризик несанкціонованого доступу і витоку конфіденційної інформації. Окрім того, важливими є поліпшити антивірусне програмне забезпечення, систему контролю доступу, процедури безпеки, системний аудит безпеки, що призведе до суттєвих позитивних змін у господарській діяльності підприємства, зокрема поліпшенні показників продуктивності та стійкості до кіберзагроз. Зазначене дає можливість запобігти значним фінансовим втратам, репутаційним ризикам та скаргам клієнтів на порушення даних (табл. 3.1).

Таблиця 3.1

Очікуване скорочення випадків витоку даних ПП «Сварожич+»

Показник	2023 р.	Прогноз на 2025 р.
Кількість випадків витоку даних	5	1
Фінансові втрати від витоків (тис. грн)	250	50
Кількість скарг клієнтів через витоки	12	2

Джерело: власні розробки.

Завдяки використанню сучасних систем виявлення та запобігання вторгненням (IDS / IPS), регулярному моніторингу кіберзагроз, незалежним аудитам безпеки та тестуванню на проникнення (пентестинг) компанії можуть виявляти та реагувати на потенційні кіберзагрози набагато швидше. Це мінімізує вплив успішної атаки, скорочує час простою та забезпечує безперервність критичних бізнес-процесів (3.2).

Таблиця 3.2

Очікуване підвищення ефективності заходів на реагування загроз

Показник	2023 р.	Прогноз на 2025 р.
Кількість успішних кібератак	3	1
Середній час реакції на загрозу (години)	5	2
Середня тривалість простою через інциденти (години)	12	4

Джерело: власні розробки.

Підвищення рівня інформаційної безпеки значно знижує ризик збоїв, простоїв і збоїв в безперервності бізнесу, пов’язаних з кібер-інцидентами і витоками даних, що сприяє підвищенню продуктивності праці, ефективності використання ресурсів і загальної конкурентоспроможності компаній на неділю (рис. 3.3).

Таблиця 3.3

Очікувані фінансово-економічні результати від впровадження заходів покращення інформаційної безпеки ПП «Сварожич+»

Показник	2023 р.	Прогноз на 2025 р.
Рентабельність активів (%)	20	24
Рентабельність власного капіталу (%)	28	32
Чистий дохід (млн. грн)	15235	17000
Частка ринку (%)	18	22

Джерело: власні розробки.

Очікується, що частка неділі збільшиться за рахунок збільшення прибутковості та чистого прибутку, підвищення довіри клієнтів та іміджу надійних партнерів. Окрім того, ПП «Сварожич+» планує запустити практику регулярних незалежних перевірок та сертифікації систем інформаційної безпеки відповідно до міжнародних стандартів, таких як ISO27001, що ще більше підвищує впевненість клієнтів, ділових партнерів і регулюючих органів в правильному рівні захисту даних на підприємстві.

Таким чином, реалізація запропонованих заходів для підвищення економічної ефективності інформаційної безпеки дозволить ПП «Сварожич+» домогтися значних поліпшень в таких важливих областях, як захист конфіденційних даних, стійкість до кіберзагроз, продуктивність праці, фінансові результати, конкурентоспроможність на ринку, що забезпечує стійке зростання компанії, підтримує її репутацію надійного партнера і сприяє реалізації стратегічних цілей розвитку бізнесу.

ВИСНОВКИ І ПРОПОЗИЦІЇ

Підприємство демонструє стабільне зростання основних фінансових показників протягом аналізованого періоду 2021-2023 рр., зокрема доходів, чистого прибутку, активів та зобов'язань, що свідчить про успішне функціонування на ринку. Показники рентабельності, такі як рентабельність активів, власного капіталу та основних фондів, мають позитивну динаміку, що підтверджує ефективне використання ресурсів підприємства. Підприємство усвідомлює важливість інформаційної безпеки та збільшує витрати на цю сферу з року в рік. Кількість успішних кібератак та час реакції на загрози зменшуються, що є ознакою вдосконалення системи інформаційної безпеки. Однак, незважаючи на зростання витрат на інформаційну безпеку, все ще спостерігається певна кількість кіберзагроз та успішних атак, що свідчить про необхідність подальшого вдосконалення системи захисту. Відсутня інформація про використання сучасних технологій та практик у сфері інформаційної безпеки, таких як багатофакторна автентифікація, шифрування даних, хмарні технології та інструменти виявлення вторгнень. Не згадується про наявність чіткої політики інформаційної безпеки, регулярних навчань для персоналу та проведення незалежних аудитів безпеки.

Для підвищення ефективності інформаційної безпеки рекомендується розробити комплексну стратегію, що охоплює технічні, організаційні та правові аспекти захисту інформації. Впровадити сучасні технології, такі як багатофакторна автентифікація, шифрування даних, системи виявлення та запобігання вторгненням, хмарні технології для резервного копіювання. Розробити чітку політику інформаційної безпеки, що визначає правила, процедури та відповідальність співробітників. Впровадити регулярні навчання для персоналу, підвищуючи обізнаність про загрози та найкращі практики. Проводити незалежні аудити безпеки та тестування на проникнення для виявлення вразливостей і своєчасного їх усунення. Розглянути можливість отримання міжнародних сертифікатів для підвищення довіри клієнтів та

партнерів до рівня захисту інформації. Впровадження цих рекомендацій допоможе підвищити ефективність інформаційної безпеки, знизити ризики витоків даних та кібератак, а також підвищити репутацію надійного партнера.

Впровадити жорсткий контроль доступу до конфіденційних даних на основі принципу «найменших привілеїв». Застосовувати сегментацію мережі та фізичне відокремлення критично важливих систем і даних. Регулярно оновлювати програмне забезпечення та операційні системи для усунення виявлених вразливостей. Впровадження цих рекомендацій допоможе суттєво підвищити ефективність захисту конфіденційних даних, забезпечити стійкість до кібератак, мінімізувати ризики витоку інформації та простоїв, а також підвищити імідж надійного партнера на ринку.

СПИСКИ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азарова А., Дьогтєва І., Шиян А. Система підтримки прийняття рішень щодо підвищення рівня інформаційної безпеки підприємства. ІТКІ. 2022. Вип. 53 (1). С. 12−18.

2. Андрущак О.І. Основи кібербезпеки. Київ: Видавництво Національного технічного університету України, 2018. 356 с.

3. Баранов О.В. Інформаційна безпека та захист даних. Харків: Видавництво Харківського національного університету радіоелектроніки, 2019. 412 с.

4. Білик В.С. Комп'ютерні мережі та їх безпека. Львів: Видавництво Львівської політехніки, 2020. 278 с.

5. Бойко С.М. Захист інформаційних систем. Одеса: Видавництво Одеської національної академії зв'язку, 2017. 384 с.

6. Вакуленко І.І. Криптографічні методи захисту інформації. Київ: Видавництво Київського національного університету ім. Т. Шевченка, 2018. 296 с.

7. Василенко А.В. Методи та засоби забезпечення інформаційної безпеки. Дніпро: Видавництво Дніпровського національного університету ім. Олеся Гончара, 2021. 352 с.

8. Гаврилюк В.В. Мережеві технології та їх безпека. Київ: Видавництво Національного авіаційного університету, 2018. 290 с.

9. Гарасюк П.М. Сучасні технології захисту інформації. Львів: Видавництво Львівської політехніки, 2019. 268 с.

10. Данилюк І.П. Інформаційна безпека: методи та засоби. Харків: Видавництво Харківського національного університету, 2020. 318 с.

11. Деркач Ю.В. Комп'ютерна безпека. Київ: Видавництво Київського національного університету будівництва і архітектури, 2017. 280 с.

12. Дорошенко О.О. Інформаційна безпека в корпоративних мережах. Дніпро: Видавництво Дніпровського державного технічного університету, 2019. 330 с.

13. Журбенко С.А. Основи інформаційної безпеки. Одеса: Видавництво Одеського національного університету ім. І.І. Мечникова, 2018. 302 с.

14. Іванов П.П. Кібербезпека та захист інформації. Харків: Видавництво Харківського національного університету внутрішніх справ, 2021. 288 с.

15. Калінін М.М. Безпека інформаційних систем. Київ: Видавництво Національного технічного університету України, 2019. 320 с.

16. Карпенко О.І. Захист інформації в комп'ютерних системах. Львів: Видавництво Львівської політехніки, 2018. 305 с.

17. Ковальчук В.М. Кіберзагрози та методи їх нейтралізації. Київ: Видавництво Національного авіаційного університету, 2020. 295 с.

18. Корчевський В.О. Криптографія та захист даних. Одеса: Видавництво Одеської національної академії зв'язку, 2017. 280 с.

19. Кузьменко С.П. Інформаційна безпека в сучасних технологіях. Дніпро: Видавництво Дніпровського національного університету ім. Олеся Гончара, 2019. 308 с.

20. Лисенко М.М. Основи кіберзахисту. Київ: Видавництво Національного технічного університету України, 2018. 272 с.

21. Лях О.В. Комп'ютерна безпека та захист інформації. Харків: Видавництво Харківського національного університету радіоелектроніки, 2019. 310 с.

22. Малишев С.М. Захист даних в інформаційних системах. Київ: Видавництво Київського національного університету ім. Т. Шевченка, 2021. 336 с.

23. Мельник В.О. Сучасні методи захисту інформації. Львів: Видавництво Львівської політехніки, 2018. 292 с.

24. Мороз В.В. Кібербезпека в корпоративних системах. Дніпро: Видавництво Дніпровського державного технічного університету, 2020. 322 с.

25. Нечипоренко П.П. Інформаційна безпека та захист даних. Харків: Видавництво Харківського національного університету, 2018. 289 с.

26. Павленко А.І. Криптографічні методи та їх застосування. Київ: Видавництво Національного технічного університету України, 2019. 305 с.

27. Петров І.В. Основи захисту інформації. Львів: Видавництво Львівської політехніки, 2017. 276 с.

28. Пономаренко О.М. Інформаційна безпека в умовах сучасних загроз. Дніпро: Видавництво Дніпровського національного університету ім. Олеся Гончара, 2020. 340 с.

29. Романенко С.С. Захист інформації в комп'ютерних мережах. Одеса: Видавництво Одеської національної академії зв'язку, 2018. 293 с.

30. Савченко В.О. Кібербезпека та інформаційний захист. Київ: Видавництво Національного авіаційного університету, 2019. 282 с.

31. Сидоренко І.М. Основи інформаційної безпеки. Харків: Видавництво Харківського національного університету внутрішніх справ, 2021. 290 с.

32. Смирнов О.О. Сучасні методи захисту даних. Київ: Видавництво Національного технічного університету України, 2018. 312 с.

33. Степаненко М.М. Комп'ютерні системи та їх безпека. Львів: Видавництво Львівської політехніки, 2019. 298 с.

34. Тараненко П.П. Інформаційна безпека в корпоративних мережах. Одеса: Видавництво Одеського національного університету ім. І.І. Мечникова, 2017. 315 с.

35. Ткаченко В.О. Кіберзагрози та їх нейтралізація. Дніпро: Видавництво Дніпровського державного технічного університету, 2020. 288 с.

36. Федоренко О.І. Основи криптографії та захисту інформації. Київ: Видавництво Київського національного університету ім. Т. Шевченка, 2018. 280 с.

37. Харченко С.С. Захист даних в комп'ютерних системах. Харків: Видавництво Харківського національного університету радіоелектроніки, 2019. 276 с.

38. Чому саме «Сварожич+». Про нас. URL: https://www.svarozhichplus.com/about-us (дата звернення: 15.05.2024).

39. Чорнобривець А.А. Кібербезпека в умовах сучасних загроз. Київ: Видавництво Національного технічного університету України, 2020. 294 с.

40. Яровенко, Г. М. Інформаційна безпека як драйвер розвитку національної економіки: дис. ... д-ра екон. наук: 08.00.03. Суми, 2021. 590 с.