МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ

Кафедра обліку і оподаткування

На правах рукопису

КОЛЕСНИК ПАВЛО АНДРІЙОВИЧ

ДИДЖИТАЛ-ТЕХНОЛОГІЇ ЦИФРОВОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОБЛІКУ ТА ОПОДАТКУВАННІ

Спеціальність: 071 «Облік і оподаткування»

Освітньо-професійна програма «Облік і оподаткування»

Робота на здобуття освітнього ступеня «Магістр»

Науковий керівник:
ФАТЕНОК-ТКАЧУК АЛЛА ОЛЕКСАНДРІВНА,
кандидат економічних наук, доцент

РЕКОМЕНДОВАНО ДО ЗАХИСТУ

Протокол № __
засідання кафедри обліку і оподаткування
від 04.12.2024 р.

Завідувач кафедри
_____ проф. Садовська І. Б.

ЛУЦЬК – 2024
Волинський національний університет імені Лесі Українки

Факультет економіки та управління
Кафедра обліку і оподаткування
Другий (магістерський) рівень
Спеціальність 071 «Облік і оподаткування»
Освітньо-професійна програма «Облік і оподаткування»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____
_____
«27» вересня 2023 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЕКТ)
ЗДОБУВАЧУ ОСВІТИ

_____ Колесника Павла Андрійовича _____
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Диджитал-технології цифрової інформаційної безпеки в обліку та оподаткуванні

Керівник проекту (роботи) Фатенок-Ткачук Алла Олексаедрівна, к.е.н., доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

2. Строк подання студентом роботи (проекту) 04.12.2024 р._____

3. Мета та завдання випускної кваліфікаційної роботи (проекту) Метою даної роботи є розробка та систематизування теоретичних положень, обґрунтування практичних рекомендацій щодо інформаційних технологій цифрової безпеки в обліку та оподаткуванні. Завдання: обґрунтувати теоретичні аспекти забезпечення безпеки цифрових даних в обліку і оподаткуванні; систематизувати показники діяльності об'єктів критичної інфраструктури задля забезпечення кіберзахисту; структурувати інструменти захисту обліково-аналітичної інформації та систематизовано напрямки вдосконалення цього процесу; розробити методичні рекомендації щодо створення системи безпеки цифрових даних в обліку і оподаткування за допомогою диджитал-технологій.

4. Дата видачі завдання 27.09.2023 р._

АНОТАЦІЯ

Колесник П. А. Диджитал-технології цифрової інформаційної безпеки в обліку та оподаткуванні.

В роботі здійснено дослідження теоретичних положень, обґрунтування практичних рекомендацій щодо диджиталізації процесу захисту цифрових даних в обліку та оподаткуванні.

У результаті ґрунтовного аналізу праць вітчизняних вчених узагальнено сутнісні характеристики процесу забезпечення безпеки цифрових даних в обліку і оподаткуванні. Уточнено сутність понять безпека даних, кібер-безпека, механізм захисту критичних підприємств. Визначено головні завдання в процесі захисту цифрових даних. Ідентифіковано та систематизовано основні методи забезпечення безпеки. Виявлено основні напрями нормативно-правового забезпечення в управлінні інформаційною безпекою у сфері обліку і оподаткування. Систематизовано показники діяльності об’єктів критичної інфраструктури задля забезпечення кіберзахисту.

У результаті аналізу внутрішнього та зовнішнього середовища досліджуваного підприємства, виявлено резерви його розвитку.

Структуровано інструменти захисту обліково-аналітичної інформації та систематизовано напрямки вдосконалення цього процесу. Ідентифіковано інструменти для захисту даних в облікових системах.

Наукова новизна одержаних результатів полягає у поглибленні окремих теоретико-методичних положень і розробленні науково-прикладних рекомендацій щодо захисту цифрової інформації в обліку та оподаткуванні. А саме: удосконалено трактування сутнісних характеристик процесу захисту цифрової інформації в обліку та оподаткуванні, що на відміну від інших базується на інформаційних технологіях безпеки. Крім того набули подальшого розвитку: сукупність методів, щодо створення системи безпеки цифрових даних в обліку і оподаткування за допомогою диджитал-технологій.

Практичне значення мають сформовані методичні рекомендації щодо створення системи безпеки цифрових даних в обліку і оподаткування за допомогою диджитал-технологій.

Ключові слова: диджитал-інструменти, цифрова безпека в обліку і оподаткуванні, комерційна таємниця, інформаційні заходи безпеки.

SUMMARY

Kolesnyk P. AND. Digital technologies of digital information security in accounting and taxation.

The work includes a study of theoretical provisions, substantiation of practical recommendations regarding the digitalization of the process of digital data protection in accounting and taxation.

As a result of a thorough analysis of the works of domestic scientists, the essential characteristics of the process of ensuring the security of digital data in accounting and taxation have been summarized. The essence of the concepts of data security, cyber security, the mechanism of protection of critical enterprises has been specified. The main tasks in the process of protecting digital data are defined. The main methods of ensuring security have been identified and systematized. The main directions of regulatory and legal support in the management of information security in the field of accounting and taxation have been identified. Performance indicators of critical infrastructure facilities to ensure cyber protection have been systematized.

As a result of the analysis of the internal and external environment of the enterprise under study, reserves of its development were revealed.

The tools for the protection of accounting and analytical information are structured and the areas of improvement of this process are systematized. Tools for data protection in accounting systems have been identified.

The scientific novelty of the obtained results lies in the deepening of certain theoretical and methodological provisions and the development of scientific and applied recommendations for the protection of digital information in accounting and taxation. Namely: the interpretation of the essential characteristics of the process of protecting digital information in accounting and taxation, which, unlike others, is based on information security technologies, has been improved. In addition, a set of methods for creating a security system for digital data in accounting and taxation with the help of digital technologies has gained further development.

Methodical recommendations on the creation of a digital data security system in accounting and taxation with the help of digital technologies are of practical importance.

Keywords: digital tools, digital security in accounting and taxation, commercial secrecy, information security measures.

ЗМІСТ

ВСТУП

Актуальність роботи. У сучасних умовах інформація стала одним із найбільш цінних ресурсів для організацій і державних установ. Зокрема, обліково-аналітичні дані, що включають фінансові, бухгалтерські та інші показники, що використовуються для прийняття управлінських рішень, є основою для функціонування бізнесу, державних органів і навіть окремих осіб. Однак із збільшенням обсягу оброблюваної інформації та розвитку новітніх технологій постає проблема захисту цих даних від різноманітних загроз. Від ефективності систем безпеки обліково-аналітичних даних залежить не лише стабільність організацій, а й безпека економічних систем на глобальному рівні.

Безпека обліково-аналітичних даних включає в себе комплекс заходів, спрямованих на запобігання несанкціонованому доступу, змінам, втратам або розголошенню інформації. Урахування сучасних технологій і зростаючих загроз, таких як кіберзлочинність, кібератаки, витоки даних, маніпуляції з інформацією, змушує організації розробляти спеціалізовані стратегії та інструменти для забезпечення захисту даних. Відсутність належного рівня безпеки може призвести до значних фінансових втрат, репутаційних збитків і навіть до втрати конкурентних переваг.

Проте навіть при застосуванні найсучасніших засобів захисту, питання забезпечення безпеки обліково-аналітичних даних залишається складним і багатогранним. Постійний розвиток технологій, зміна форм загроз і необхідність адаптації до нових умов вимагатимуть від організацій постійного вдосконалення систем безпеки. У зв'язку з цим, інтерес до інструментів і методів забезпечення безпеки цих даних є надзвичайно актуальним у сучасному інформаційному середовищі.

Проблеми обліково-аналітичного захисту обліково-аналітичної інформації, у системі управління підприємством знайшли відображення в працях вітчизняних та іноземних вчених, а саме: О. А. Баранова, К. П. Боримської, С. І. Василішина, С. М. Деньги, З.-М. Задорожного, З. Б. Живко, А. О. Фатенок-Ткачук.

Незважаючи на ґрунтовний доробок, потребують уточнення методичні аспекти захисту обліково-аналітичної інформації та їх відображення в обліковій політиці підприємства.

Багато науковців вважають, що до сьогоднішнього дня питання однозначного розуміння сутності та основне методики забезпечення безпеки цифрових даних в обліку і аудиті не існує через відсутність нормативного забезпечення, тому все ще залишаються відкритими та потребують вирішення окремі питання.

Мета і завдання дослідження. Метою даної роботи є розробка та систематизування теоретичних положень, обґрунтування практичних рекомендацій щодо процесу диджиталізації безпеки цифрової інформації в обліку та оподаткуванні.

Для досягнення мети поставлено та вирішено **такі завдання**:

- обґрунтувати теоретичні аспекти процесу захисту цифрової інформації в обліку та оподаткуванні;
- розкрити та уточнити сутність понять цифрова інформація, безпека даних, кібер-безпека;
- виявити напрями нормативно-правового забезпечення в управлінні інформаційною безпекою у сфері обліку і оподаткування;
- систематизувати показники діяльності об’єктів критичної інфраструктури задля забезпечення кіберзахисту;
- здійснити аналіз внутрішнього та зовнішнього середовища досліджуваного підприємства з метою виявлення резервів розвитку;
- структурувати інструменти захисту обліково-аналітичної інформації;
- систематизувати напрямки вдосконалення процесу захисту цифрової інформації в обліку та оподаткуванні;
- розробити методичні рекомендації щодо створення системи безпеки цифрових даних в обліку і оподаткування за допомогою диджитал-технологій;
- ідентифікувати інструменти для захисту даних в облікових системах.

Об’єктом дослідження є процес захисту цифрової інформації в обліку та оподаткуванні.

Предметом дослідження – теоретичні, методичні та прикладні положення з забезпечення захисту цифрової інформації в обліку та оподаткуванні.

Методи дослідження. У роботі використовувались загальноекономічні, статистичні, розрахунково-аналітичні, математичні методи дослідження.

Інформаційними джерелами для написання кваліфікаційної роботи стали: законодавчі та нормативні акти, наукові статті, автореферати до дисертацій, монографії, дані фінансової звітності досліджуваного підприємства.

Наукова новизна одержаних результатів полягає у поглибленні окремих теоретико-методичних положень і розробленні науково-прикладних рекомендацій щодо захисту цифрової інформації в обліку та оподаткуванні. Основні положення наукової роботи полягають у такому:

удосконалено: трактування сутнісних характеристик процесу захисту цифрової інформації в обліку та оподаткуванні, що на відміну від інших базується на інформаційних технологіях безпеки.

набули подальшого розвитку: сукупність методів, щодо створення системи безпеки цифрових даних в обліку і оподаткування за допомогою диджитал-технологій.

Практичне значення одержаних результатів полягає у тому, що рекомендації і пропозиції, а також розробки, наведені в роботі, сприяють розвитку обліково-аналітичного забезпечення стратегій розвитку вітчизняних підприємств, зокрема у діяльності ХХХХХХХХХХХХХХХ (акт про впровадження № 123 від 20.11.2024 р.).

Апробація результатів дослідження. Основні положення кваліфікаційної роботи магістра доповідались на міжнародних конференціях, зокрема V науково-практичній міжнародній інтернет-конференції молодих науковців, здобувачів освіти «Сучасні тенденції розвитку обліку, аналізу, контролю, аудиту та оподаткування» (21 листопада 2024 р., м. Луцьк).

Публікації. Основні наукові положення кваліфікаційної роботи магістра опубліковано в 1 тезах міжнародної наукової конференцій. Загальна кількість публікацій за темою магістерської роботи становить 1 праця.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ДИДЖИТАЛ-ТЕХНОЛОГІЙ ЦИФРОВОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОБЛІКУ ТА ОПОДАТКУВАННІ

1.1 Теоретичні основи диджитал-технологій цифрової інформаційної безпеки

Однією з основних задач забезпечення безпеки обліково-аналітичних даних є створення багаторівневої системи захисту, яка включає як технічні, так і організаційні заходи. На технічному рівні використовуються різноманітні інструменти шифрування, засоби аутентифікації та управління доступом, системи моніторингу і виявлення загроз. Організаційні заходи включають розробку політик безпеки, регулярне навчання персоналу та створення системи реагування на інциденти.

Правове регулювання безпеки даних має величезне значення в забезпеченні належного рівня захисту обліково-аналітичної інформації. Національні та міжнародні нормативно-правові акти, стандарти та рекомендації визначають обов'язкові вимоги щодо зберігання, обробки та передачі даних, забезпечуючи тим самим правову основу для реалізації політик інформаційної безпеки. Невиконання цих вимог може призвести до юридичних санкцій і серйозних економічних наслідків для організацій. Розглянемо сутнісні характеристики досліджуваного питання.

Інформаційна безпека – це безпека будь-якої інформації, включаючи паперові документи, голосову інформацію тощо. До неї часто відносять питання державної безпеки, пропаганди, цензури, соціальних маніпуляцій тощо. Крім того до інформаційної безпеки (ІБ) часто відносять фізичну безпеку, безпеку персоналу, безпеку відносин із третіми сторонами, безперервність бізнесу тощо. Прикладом такого бачення є міжнародний стандарт із управління безпекою організацій ISO 27001.

Інформаційна безпека є основою економічної безпеки підприємства.

Сьогодні термін «безпека» розглядається як одна з ключових проблем, яка зачіпає кожного індивіда, підприємства, регіони, держави та світову спільноту в цілому. Це поняття постійно еволюціонує, його зміст ускладнюється та набуває нових відтінків.

Згідно з тлумачним словником В. Даля, «безпека» означає збереження, надійність та відсутність загроз як для особистості, так і для суспільства та держави. У сучасному розумінні безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства чи організації від потенційних і реальних загроз, або ж повна їх відсутність.

У Західній Європі термін «безпека» почав використовуватись ще в XII столітті, проте значного поширення набув лише у XVII–XVIII століттях, коли основним завданням держави вважалося забезпечення добробуту та захисту від загроз. У ті часи безпеку визначали як стан, в якому небезпеки усунуто або нейтралізовано, а соціальні інститути забезпечують стабільність.

В епоху Російської імперії термін «безпека» став застосовуватись для позначення охорони громадського порядку, зокрема через активізацію революційної діяльності. У 1881 році було запроваджено «Положення про заходи щодо охорони державного порядку та громадського спокою», в якому вперше визначено поняття «громадська безпека».

Безпека розглядається як стан, що дозволяє ефективно запобігати зовнішнім та внутрішнім загрозам, забезпечувати стабільний розвиток об’єкта та його гармонійне існування. Це поняття багатогранне й застосовується на різних рівнях: від глобального та міжнародного до індивідуального.

На міжнародному рівні безпека передбачає гарантії для окремих держав і їхніх суб’єктів. Розширення інтеграційних зв’язків між країнами формує умови для економічного співробітництва, водночас впливаючи на внутрішні політики окремих держав.

На національному рівні безпека охоплює економічну стабільність та захист інтересів країни, що можливе завдяки участі в міжнародному поділі праці, сталому соціально-економічному розвитку та ефективній співпраці на світовій арені. Основним документом, який регулює державну політику в цій сфері, є

Закон України «Про національну безпеку», ухвалений 21 червня 2018 року. Координацію питань безпеки здійснює Рада національної безпеки і оборони України.

Поняття «економічна безпека» вперше ввів у вжиток Ф. Рузвельт близько 90 років тому, а офіційно його закріплено в 1985 році в резолюції Генеральної Асамблеї ООН «Міжнародна економічна безпека». Економічна безпека має особливе значення, оскільки всі інші види безпеки безпосередньо залежать від економічного забезпечення. Стабільна система економічної безпеки є фундаментом для захисту національних інтересів та забезпечення незалежності держави [1].

У сучасній економічній науці існує безліч підходів до визначення економічної безпеки держави. Проте часто увага акцентується лише на інтересах людини, суспільства та держави, тоді як потреби підприємств — основних складових економіки – залишаються недостатньо врахованими.

Економічна безпека регіону, за визначенням З. Герасимчук і Н. Вавдіюк, характеризується станом, у якому регіон досягає максимально ефективного та раціонального використання свого економічного потенціалу, забезпечує захист від дестабілізуючих впливів, підтримує стабільні внутрішні зв’язки, що дозволяє задовольняти соціально-економічні потреби мешканців у рамках загальнодержавних інтересів [2].

Безпека підприємства відіграє центральну роль у загальній ієрархії рівнів безпеки. Підприємство – ключова ланка економіки, яка впливає на розвиток не лише окремих регіонів, але й держави в цілому. Стійкий розвиток, ефективність функціонування та конкурентоспроможність підприємств значною мірою залежить від рівня захищеності їхньої діяльності. Поняття безпеки підприємства охоплює фінансову стабільність, інформаційний захист, збереження майна, охорону інтелектуальних прав і посадових осіб.

Підприємницька діяльність завжди приваблює антисуспільні явища, такі як корупція, шахрайство, рейдерство чи недобросовісна конкуренція. В умовах постійних зовнішніх і внутрішніх загроз ключовою метою підприємств стає створення ефективної системи економічної безпеки. Сучасні реалії вимагають від

підприємств активного залучення фахівців у цій сфері, оскільки потреба у забезпеченні захищеності зростає.

Перші українські наукові роботи, присвячені економічній безпеці підприємств, з'явилися в середині 90-х років XX століття. Початково це поняття зводилося до захисту комерційної інформації. Наразі ж воно стало набагато ширшим, охоплюючи різноманітні аспекти діяльності підприємств.

Основні підходи до визначення економічної безпеки підприємства:

Ресурсно-функціональний підхід. Цей підхід, популяризований Є. Олейніковим, розглядає економічну безпеку як стан оптимального використання ресурсів (капітал, персонал, інформація, технології), що забезпечує стійкість підприємства та протидію загрозам. Аналогічну позицію поділяють С. Ф. Покропивний та Т. Б. Кузенко, ототожнюючи економічну безпеку з ефективністю діяльності підприємства [3].

Адаптивно-захисний підхід. Згідно з Д. Ковальовим і Т. Сухоруковою, економічна безпека визначається як захищеність підприємства від негативних впливів зовнішнього середовища та здатність адаптуватися до змін. Однак цей підхід має недоліки, оскільки обмежується зовнішніми факторами, ігноруючи внутрішні, такі як кадровий потенціал чи технічна оснащеність.

Інтеграційний підхід. Цей підхід акцентує на гармонізації інтересів підприємства із зовнішніми суб'єктами, з якими воно взаємодіє. Представники підходу, зокрема Г. В. Козаченко, О. М. Ляшенко та В. П. Пономарьов, розглядають економічну безпеку як інструмент забезпечення сталого розвитку шляхом інтеграції інтересів у просторі й часі [4].

Дослідження економічної безпеки підприємства є складним завданням через необхідність врахування багатьох аспектів, зокрема гармонізації інтересів підприємства та суб'єктів зовнішнього середовища. Проблема полягає у значній різноманітності цих інтересів, серед яких чимало мають опосередкований вплив на діяльність підприємства.

Основні підходи до визначення економічної безпеки підприємства:

Захист інтересів і ресурсів підприємства. А. С. Соснін і П. Я. Пригунов трактують економічну безпеку як захист життєво важливих і законних інтересів

підприємства від внутрішніх та зовнішніх загроз у різних протиправних формах, що сприяє його стабільному розвитку.

Стан діяльності та господарських відносин. Прихильники цього підходу (О. Ф. Долженков, Ж. О. Жуковська, О. М. Головченко) визначають економічну безпеку як стан юридичних і виробничих відносин, що забезпечують ефективне функціонування, фінансовий успіх, науково-технічний та соціальний розвиток підприємства.

Забезпечення умов для функціонування. Інші дослідники, такі як О. Раздіна і Н. Капустін, акцентують увагу на методах, засобах і факторах, які створюють умови для ефективної роботи підприємства.

Динамічний підхід. О. В. Ареф'єва та Р. М. Федоренко підходять до визначення економічної безпеки як динамічного стану, що дозволяє підприємству адаптуватися до змін зовнішнього та внутрішнього середовища, забезпечуючи його стратегічний розвиток.

Фінансово-економічна безпека підприємства розглядається як інтегроване поняття, що об'єднує економічні та фінансові аспекти. Це підкреслює взаємозалежність фінансової та економічної діяльності підприємств. Науковці (Н. Ю. Подольчак, В. Я. Карковська) визначають її як захищеність потенціалу підприємства у різних сферах від негативних впливів, здатність до відтворення та протистояння загрозам [5].

Ключові характеристики економічної безпеки підприємства: висока ефективність використання корпоративних ресурсів; комплексність, що охоплює всі напрямки діяльності підприємства; залежність від зовнішніх і внутрішніх факторів, таких як податкова політика, бізнес-процеси, взаємодія з постачальниками і клієнтами; взаємозв'язок із конкурентоспроможністю підприємства та безпекою держави.

Інформаційна безпека є важливою складовою національної безпеки, яка спрямована на захист національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз. Вона охоплює захист інформаційного простору, національних інформаційних ресурсів, а також забезпечення безпечного функціонування інформаційних і телекомунікаційних систем. Інформаційна

безпека також включає захист інформації, яка циркулює в цих системах, та забезпечення захисту свідомості та психіки людей від небажаних інформаційних впливів.

Класифікація видів загроз в інформаційній безпеці: забезпечення свободи слова і доступу до інформації, протидія маніпуляціям з інформацією, в тому числі фальшивими новинами; протидія поширенню інформації, що пропагує насильство, жорстокість, порнографію; захист від комп'ютерної злочинності та тероризму, включаючи боротьбу з кіберзлочинами; захист інформаційно-телекомунікаційних систем від атак і забезпечення безпеки для державних органів і сфер економіки; захист національних інформаційних ресурсів, зокрема тих, що доступні через Інтернет.

Державна політика у сфері інформаційної безпеки повинна зосереджуватись на: створенні та забезпеченні функціонування цілісної системи інформаційної безпеки в Україні; розробці та впровадженні новітніх інформаційних технологій для захисту інформаційної інфраструктури; вдосконаленні нормативно-правової бази в галузі інформаційної безпеки.

Таким чином, ефективне забезпечення інформаційної безпеки потребує комплексного підходу, що включає стратегічне планування, правову та організаційну підтримку, а також технологічні заходи для захисту національних інтересів у цифровому середовищі.

Основними принципами ІБ є – цілісність, доступність і конфіденційність. Ці вимоги застосовні не тільки до електронної інформації, але й до «паперової», усної тощо.

Безпека ІТ (комп’ютерна безпека, цифрова безпека, ІТ-безпека) це – захист від хакерів, вірусів, спаму, фішингу та безлічі інших загроз, що виникають, головним чином, з Інтернету. Цей захист найчастіше реалізується зниженням тих чи інших організаційних або технічних вразливостей безпеки.

Безпека ІТ – це забезпечення цілісності, доступності, конфіденційності та інших вимог безпеки, що пред’являються до обчислювальної та комунікаційної техніки та інформації, яку вона зберігає, обробляє та передає. До завдань безпеки ІТ відносять також захист від соціальної інженерії, управління ефективністю

безпеки, надання гарантій безпеки, відповідності нормативним вимогам безпеки, страхування інформаційних ризиків, забезпечення безперервності бізнесу.

Поняття кібер-безпеки започатковане від теміну “кібернетика”. Він був придуманий Андре-Марі Ампером у 1834 році та розвинений Норбертом Вінером у 1948 році. Кібернетика в сучасному розумінні – це дисципліна про інформацію в складних керуючих системах. Наприклад, у комп’ютері, людині чи суспільстві.

У сучасному контексті приставка «кібер-» набула широкого поширення та переосмислення завдяки канадсько-американському письменнику-фантасту Вільяму Гібсону. У 1984 році у своєму романі «Нейромант» він запровадив та популяризував термін «кіберпростір» (cyberspace) для опису віртуальної реальності та глобальних комунікаційних мереж. Його роботи вплинули на масову культуру і сформували сучасне розуміння цифрового світу.

Вільям Гібсон використав приставку «кібер-» саме через її позитивний, організуючий сенс, щоб підкреслити контраст між ідеалами управління і тими антиутопічними реаліями, які можуть виникнути при неконтрольованому розвитку технологій. Його роботи послужили нагадуванням про подвійну природу прогресу: технології мають потенціал як для поліпшення життя, так і для створення нових форм ризику та нерівності. Вибір приставки “кібер” був усвідомленим художнім прийомом, що дозволяє глибше дослідити теми контролю, свободи та людської сутності в епоху стрімкого технологічного розвитку.

В результаті приставка «кібер-» почала асоціюватися з цифровими технологіями, комп’ютерами та Інтернетом.

Кібербезпека в сучасному розумінні – це захист цифрових систем, мереж та даних від кіберзагроз, що виходять із кіберпростору. Вона фокусується на запобіганні кібератакам, несанкціонованому доступу, крадіжці даних та іншим цифровим загрозам.

Технічно, коли в поєднанні зі словом “безпека” ми вживаємо слово “кібер”, що означає по-грецьки “кермовий на судні” або “уряд”, ми за фактом говоримо про “руління”, тобто про управління безпекою.

Повертаючись до кібернетики, під кібербезпекою можна мати на увазі

безпеку інформації в складних системах управління. У той же час, така безпека сама по собі є складною підсистемою управління. Тому у будь-якому випадку справа зводиться до управління безпекою.

Виходить, якщо розібратися у витоках, кібер-безпека – це управління інформаційною безпекою в розумінні все того ж стандарту ISO 27001. Тобто, це набір процесів і засобів управління інформаційною безпекою.

Таким чином, ми спробували неупереджено розібратися у відмінностях інформаційної безпеки, IT-безпеки та кібербезпеки. Не дарма кожне з цих понять пов'язане з управлінням безпекою. Саме грамотне управління надає безпеці цінність. Найпоширенішим стандартом такого управління є ISO 27001. Його значення в сучасній інформаційній безпеці важко переоцінити. Цей стандарт є основою багатьох інших державних і галузевих стандартів інформаційної безпеки [41].

1.2 Нормативне забезпечення в управлінні інформаційною безпекою у сфері обліку і оподаткування

Основним нормативно-правовим інструментом управління інформаційною безпекою є Міжнародний стандарт ISO 27001 [42]. Він зосереджений на ідентифікації, оцінці та управлінні ризиками для процесів обробки інформації. Безпека конфіденційної інформації підкреслюється як важливий стратегічний елемент.

Інформація оточує нас всюди і є частиною кожного процесу. Іноді це може бути незначущим, але дуже часто це критично й конфіденційно. Щоб скористатися цією важливою відмінністю для вашої організації, необхідно класифікувати інформацію. Це пояснюється тим, що захисні заходи системи управління інформаційною безпекою (СУІБ - ISMS) відповідно до ISO/IEC 27001 засновані на цій класифікації.

СУІБ створює основу для захисту оперативних даних та їх конфіденційності. Водночас визнаний у світі стандарт забезпечує доступність IT-

систем, задіяних у корпоративних процесах. У цьому контексті сертифікація ISO 27001 посилає сильний сигнал ринку: а саме незалежну зовнішню оцінку та підтвердження ефективності вашої СУІБ.

З EN ISO/IEC 27001:2017-06 була опублікована версія, координована Європейським комітетом стандартизації (CEN). Вона поєднує два виправлення (корригенди) Cor 1:2014 та Cor 2:2015. Зміни, пов’язані з виправленням, включають лише покращений опис пов’язаних вимог, але не містять нових додаткових вимог. Таким чином, сертифікати відповідно до версії ISO/IEC 27001:2013 зберігають свою дію.

Стандарт ISMS ISO 27001 діє у всьому світі. Він надає компаніям усіх розмірів і галузей основу для планування, впровадження та моніторингу їх інформаційної безпеки. Вимоги поширюються на приватні та державні компанії, а також некомерційні організації.

У Німеччині, наприклад, компанії, які належать до сектору критичної інфраструктури (KRITIS) і перевищують поріг, повинні надати докази того, як вони забезпечують свою інформаційну безпеку. Сектори KRITIS включають енергетику, воду, охорону здоров'я, фінанси та страхування, харчування, транспорт і рух, інформаційні технології та телекомунікації. Відповідне підтвердження впровадження може бути надане аудитом безпеки, випробуванням або сертифікацією. Для цього в якості основи для аудиту можна використовувати визнані стандарти, наприклад ISO 27001, або галузеві стандарти безпеки, визнані Федеральним відомством інформаційної безпеки Німеччини (BSI).

Завдяки своїм потужним фінансовим, технологічним, науково-технічним і військовим ресурсам, а також значній увазі, що приділяється національній безпеці, захисту громадянських прав і інтересів бізнесу, досвід США в управлінні інформаційною безпекою є надзвичайно важливим для вивчення. Значення цього досвіду на державному рівні ще більше підкреслюється концентрацією в країні провідних фінансових установ, дослідницьких організацій і корпорацій, які відіграють ключову роль у розвитку технологій, фінансовій стабільності та економічному прогресі на глобальному рівні.

Одним із важливих напрямків розвитку інформаційної безпеки в США є забезпечення національної безпеки, зокрема захисту інформаційних систем державних «силових» структур, таких як збройні сили, зовнішня розвідка та інші критичні відомства. Вже з 1992 року Міністерство оборони США активно працювало над організацією заходів у сфері інформаційної безпеки в рамках концепції «Інформаційного протиборства». Ця концепція була спрямована на вирішення завдань з боротьби з системами управління збройними силами супротивника на різних рівнях, а також на забезпечення безпеки та ефективності власних інформаційних систем армії США. У 1996 році ця концепція отримала подальший розвиток у вигляді нового польового статуту армії США «Інформаційні операції», що стало важливим кроком у напрямку удосконалення інформаційної безпеки [16].

Розвиток системи національної інформаційної безпеки отримав новий імпульс з виданням директиви Presidential Decision Directive 63 (PDD 63) адміністрацією президента Білла Клінтона 22 травня 1998 року, що зосередилася на захисті критично важливої інфраструктури США. Цей документ став основою для підписаного Біллом Клінтоном на початку 2000 року «Загальнонаціонального плану захисту інформаційних систем», який визначив ключові напрямки державної політики в галузі інформаційної безпеки. Після цього в лютому 2003 року адміністрація президента Джорджа Буша-молодшого опублікувала «Національну стратегію досягнення безпеки в кіберпросторі», в якій визначено п’ять пріоритетів щодо забезпечення інформаційної безпеки та основні завдання в рамках цих пріоритетів на середньострокову та довгострокову перспективу.

Ці документи стали основою для формування офіційної загальнонаціональної політики США в галузі інформаційної безпеки, яка визначає структуру державної діяльності і відповідних органів, що займаються питаннями безпеки на національному рівні.

Основними пріоритетами цієї стратегії є:

- Створення та розвиток національної системи реагування на інциденти в сфері інформаційної безпеки, що дозволяє швидко і ефективно реагувати на

будь-які загрози.

- Реалізація комплексних заходів для зниження ризиків і загроз для інформаційної безпеки, зокрема через розробку і впровадження передових технологій захисту.
- Підготовка висококваліфікованих фахівців у сфері комп'ютерної безпеки, а також формування відповідального ставлення до питань захисту інформації серед усіх громадян.
- Захист інформаційних систем, що мають стратегічне значення для держави, зокрема в урядових структурах і критичних інфраструктурах.
- Розвиток форм міжнародної кооперації у сфері інформаційної безпеки, що є важливим для протидії транснаціональним кіберзагрозам та забезпечення глобальної стабільності в кіберпросторі.

Таким чином, стратегія США в галузі інформаційної безпеки є комплексним підходом, який охоплює всі аспекти захисту інформаційних ресурсів на національному та міжнародному рівнях. Це дозволяє країні не лише забезпечувати безпеку своїх критичних систем, а й активно брати участь у формуванні глобальних стандартів і практик у цій сфері.

Пріоритет 1. Розвиток системи реагування на події в сфері інформаційної безпеки.

Швидке виявлення кіберзагроз та своєчасний обмін інформацією про них є критично важливими для мінімізації збитків від атак. Для досягнення цієї мети Стратегія передбачає кілька основних заходів:

- Розробка архітектури взаємодії між урядовими і неурядовими структурами, що дозволить оперативно реагувати на інциденти в сфері інформаційної безпеки.
- Впровадження системи як тактичного, так і стратегічного аналізу атак на інформаційні ресурси для оцінки їх вразливості та розробки відповідних заходів.
- Заохочення приватних компаній до активного обміну інформацією про стан справ в інформаційній безпеці, що дозволить покращити загальну

обізнаність про поточні загрози та вразливості.

Пріоритет 2. Усунення загроз для інформаційної безпеки та вразливостей в інформаційних системах.

Наявність вразливостей у різних інформаційних системах може стати каталізатором для атак, що створює серйозні загрози для критично важливих об'єктів інфраструктури. Тому усунення цих вразливостей є одним з ключових завдань у сфері інформаційної безпеки. Стратегія передбачає такі основні заходи: розширення можливостей для проведення розслідувань комп'ютерних злочинів, що дозволить запобігти подібним інцидентам у майбутньому; створення загальнонаціонального механізму для оцінки вразливостей, що забезпечить краще розуміння негативних наслідків від використання цих вразливостей; покращення безпеки Інтернету шляхом вдосконалення протоколів і механізмів маршрутизації, що сприятиме більш ефективному захисту від атак.

Пріоритет 3. Розвиток відповідального ставлення до інформаційної безпеки та підготовка кадрів.

Недостатнє розуміння важливості захисту інформаційних систем серед користувачів, адміністраторів і розробників є джерелом багатьох вразливостей. Стратегія передбачає наступні заходи для підвищення обізнаності та підготовки кадрів: реалізація загальнонаціональної програми, яка популяризує відповідальне ставлення до забезпечення безпеки інформаційних систем серед громадян; заохочення створення навчальних програм, що забезпечать розвиток необхідних навичок і компетенцій у фахівців; підвищення ефективності існуючих програм підготовки професіоналів у галузі інформаційної безпеки; підтримка приватних компаній у створенні сертифікаційних програм для підвищення кваліфікації та створення загального визнання цих сертифікатів на ринку праці.

Пріоритет 4. Охорона державних інформаційних ресурсів.

Забезпечення безпеки інформаційних ресурсів держави є однією з головних задач для захисту національних інтересів. Для цього Стратегія передбачає:

Постійне оцінювання загроз для державних інформаційних систем і вразливостей, що можуть виникнути внаслідок цих загроз.

Захист бездротових урядових мереж, що є важливими для стабільного функціонування державних структур.

Забезпечення безпеки в процесах аутсорсингу та закупівель для державних потреб, щоб мінімізувати ризики у співпраці з третіми сторонами.

Пріоритет 5. Розвиток кооперації між різними відомствами та міжнародної кооперації у сфері інформаційної безпеки.

Інформаційні системи є глобально взаємопов’язаними, тому для ефективного захисту необхідно застосовувати системний підхід. Стратегія передбачає такі важливі заходи:

Посилення контррозвідувальної діяльності в сферах, пов'язаних з інформаційними системами і технологіями, для запобігання кіберзагрозам.

Створення національних та міжнародних мереж спостереження і попередження атак на інформаційні ресурси, що дозволяє оперативно виявляти загрози [17-19].

Заохочення інших країн до приєднання до Конвенції Ради Європи з кіберзлочинів або вдосконалення національних законодавств у галузі кібербезпеки для підвищення глобальної безпеки в цій сфері.

Ці пріоритети формують основну основу для збереження безпеки інформаційних систем як на національному, так і на міжнародному рівнях, дозволяючи ефективно реагувати на загрози і підвищувати стійкість до атак.

Згідно з загальною політикою та наявною інфраструктурою управління в США, було створено ефективну систему державних органів, що займаються забезпеченням інформаційної безпеки. Ця система постійно удосконалюється та включає різні органи, які реалізують заходи на всіх рівнях управління, починаючи від національного до регіонального.

Одним з основних органів, спеціально створених для вирішення завдань у сфері інформаційної безпеки, є Комітет з національних систем безпеки (Committee on National Security Systems, CNSS), який відіграє важливу роль у формулюванні політики та координації дій між різними установами.

У рамках виконавчої влади США були також створені нові спеціалізовані

федеральні установи, основним завданням яких є забезпечення національної безпеки та вирішення проблем інформаційної безпеки на федеральному рівні. До таких установ відносяться:

Міністерство національної безпеки (Department of Homeland Security, DHS), яке відповідає за координацію заходів щодо захисту критично важливих інфраструктур та ресурсів країни.

Управління внутрішньої безпеки (Office of Homeland Security), яке забезпечує розробку та впровадження національних планів реагування на інциденти в сфері інформаційної безпеки.

Рада з внутрішньої безпеки (Homeland Security Council), яка здійснює координацію політики в галузі захисту інформаційних систем та критичних інфраструктур, що мають стратегічне значення для національної безпеки.

Основною причиною інтеграції функцій із забезпечення інформаційної безпеки до складу Міністерства національної безпеки та інших органів є зростаюча загроза, яку несуть кібер-атаки для стратегічних секторів економіки США, таких як фінансовий, енергетичний, транспортний та інші, що можуть мати далекосяжні наслідки для національної безпеки.

Зокрема, для вирішення конкретних завдань у сфері кібербезпеки, в різних федеральних органах були створені спеціалізовані підрозділи, що займаються безпекою інформаційних систем:

United States Computer Emergency Readiness Team (US-CERT), що функціонує в складі DHS і відповідає за реагування на інциденти в інформаційних системах, включаючи розслідування кібер-атаки та їх наслідки.

Army Global Network Operations and Security Center (AGNOSC) – підрозділ Міністерства оборони США, який координує забезпечення безпеки глобальних мереж армії та надає підтримку у захисті інформаційних ресурсів.

Defense Information Systems Agency (DISA) – підрозділ Міністерства оборони США, який керує діяльністю Joint Task Force for Computer Network Operations (JTF-CNO) для захисту комп’ютерних мереж, що обслуговують збройні сили [20].

National Security Agency (NSA), що через Central Security Service (CSS) займається захистом національних інформаційних систем і здійснює розвідку в кіберпросторі для попередження кібер-загроз.

Ця складна мережа організацій та спеціалізованих підрозділів забезпечує високий рівень координації та взаємодії між різними секторами влади, що дозволяє ефективно реагувати на сучасні виклики в сфері інформаційної безпеки і кіберзахисту.

У системі забезпечення інформаційної безпеки США роль різних державних органів та їх координація є ключовими для ефективного реагування на кіберзагрози та управління національною інформаційною інфраструктурою. Комітет з національних систем безпеки (CNSS), який складається з 21 члена та 11 спостерігачів з федеральних установ, виконує важливу роль у формуванні державної політики у сфері інформаційної безпеки. Основні напрямки його діяльності включають управління ризиками, стійкість мережевої інфраструктури, розвиток системи підготовки кадрів та забезпечення надійності інформаційних ресурсів [21].

CNSS розробляє національну політику та стандарти для забезпечення захисту інформації, проводить оцінку засобів захисту, а також видає директиви та інструкції щодо безпеки інформаційних систем. Крім того, комітет бере участь у регулюванні експорту засобів захисту інформації.

Міністерство національної безпеки (DHS) має важливі функції у сфері інформаційної безпеки, зокрема розробку та вдосконалення національних планів безпеки, управління кризовими ситуаціями, а також надання технічної підтримки приватним компаніям та урядовим організаціям. В рамках DHS функціонує Управління кібербезпеки та комунікацій (Office of Cyber Security and Communications), яке відповідає за захист критично важливих інфраструктур та реалізацію заходів щодо усунення наслідків кіберінцидентів через підрозділ National Cyber Security Division, до якого входить US-CERT.

US-CERT займається реагуванням на інциденти в сфері інформаційної безпеки та взаємодіє з урядовими та приватними структурами для зниження

вразливості критично важливих інфраструктур. Внутрішні підрозділи US-CERT включають відділи для аналізу інцидентів, ситуаційної поінформованості, слідства, перспективного розвитку та підтримки. Для забезпечення готовності до надзвичайних ситуацій в інформаційній безпеці, DHS організовує навчання Cyber Storm, координує роботу з 13 федеральними відомствами та підтримує систему обміну інформацією через Cyber Cop Portal.

Агентство оборонних інформаційних систем (DISA) в межах Міністерства оборони США координує забезпечення безпеки інформаційних систем військового відомства через Joint Task Force for Computer Network Operations (JTF-CNO). Це агентство виявляє вторгнення в оборонні мережі, оцінює їх вплив на військові операції та організовує відновлення роботи мереж [22].

1.3 Кіберзахист об’єктів критичної інфраструктури у контексті безпеки цифрових даних

Стан у якому на сьогодні працюють суб’єкти господарювання супроводжується постійними кібератаками як на самі підприємства так і сукупність їх цифрових даних в сфері обліку та оподаткування. Визнання підприємства частиною критичної інфраструктури спрошує військовий облік та сприяє безперервному випуску продукції важливої для існування громадян України. У зв’язку з виникненням нового формату підприємств виникла необхідність нормативного забезпечення їх діяльності та обліку. Так у 2019 році Кабміном було прийнято постанову про затвердження «Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [43]. Саме вони є основою організації захисту обліково-аналітичної інформації на сьогодні.

Критичні бізнес/операційні процеси об’єкта критичної інфраструктури – процеси організації функціонування об’єктів критичної інфраструктури, реалізація загроз на які призводить до виведення з ладу або порушення функціонування самого об’єкта критичної інфраструктури та відповідно справляє

негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіює майнову шкоду та/або становить загрозу для суспільства, життя і здоров'я людей; для організації функціонування цього процесу можуть використовуватися декілька інформаційно-комунікаційних систем.

Система інформаційної безпеки – сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються), запобігання порушенню режиму функціонування та/або недоступності служб (функцій) об'єкта критичної інформаційної, порушенню функціонування компонентів об'єкта; забезпечення спостережності за діями користувачів та функціонуванням засобів захисту об'єкта критичної інформаційної інфраструктури.

На таких об'єктах має діяти політика інформаційної безпеки. Політика інформаційної безпеки – політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки.

Організаційні та технічні заходи з кіберзахисту, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, повинні забезпечувати: формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки; управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури; ідентифікацію та автентифікацію користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури; реєстрацію подій компонентами об'єкта критичної інформаційної інфраструктури об'єкта

критичної інфраструктури та їх періодичний аудит; мережевий захист компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури; доступність та відмовостійкість компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури; визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури; визначення умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури; визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Під час доповнення переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури для кожної загрози об’єкта критичної інформаційної інфраструктури передбачаються захід або комплекс заходів, що забезпечують блокування однієї чи декількох загроз або знижують ризик її реалізації, та враховуються умови функціонування

Формування додаткових заходів із забезпечення кіберзахисту розробник комплексної системи захисту інформації здійснює з урахуванням вимог нормативних документів у сфері технічного захисту інформації, міжнародних стандартів з питань інформаційної безпеки.

Об’єкт критичної інфраструктури повинен мати у своєму складі підрозділ або посадову особу з інформаційної безпеки, що відповідають за політику інформаційної безпеки, прийняту на підприємстві та контроль за її дотриманням. Під час визначення відповідальних за інформаційну безпеку перевага повинна надаватися особам, які мають фахову освіту та досвід роботи у сфері технічного захисту інформації або інформаційної безпеки. Крім того мають бути визначені права та обов’язки всіх категорій користувачів та адміністраторів інформаційної інфраструктури, обов’язки адміністраторів з обслуговування компонентів та забезпечення її інформаційної безпеки, які оформлюються окремим рішенням.

Рекомендовано для підприємств мати визначений перелік інформаційних,

програмних та апаратних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта, рівень їх критичності та можливий рівень наслідків у випадку порушення конфіденційності, цілісності та доступності інформації, недоступності служб (функцій) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, порушення функціонування компонентів об’єкта.

На об’єкті критичної інфраструктури повинно бути затверджено політику управління ризиками інформаційної безпеки і методику їх оцінювання та оброблення. Методичною основою для вибору методики є стандарт ДСТУ ISO/IEC 27005.

Виконання переліку обов’язкових правил кібербезпеки сприятимуть захисту обліково-аналітичної інформації підприємства.

РОЗДІЛ 2
АНАЛІЗ ВНУТРІШНЬОГО СЕРЕДОВИЩА ЗАДЛЯ МОЖЛИВОСТІ РОЗВИТКУ ДИДЖИТАЛ-ТЕХНОЛОГІЙ ЗАХИСТУ ЦИФРОВИХ ДАНИХ ПІДПРИЄМСТВА

2.1 Аналіз тенденцій розвитку виробництва торговельного обладнання в Україні

Важливою складовою стратегічного планування для підприємств, які спеціалізуються на виробництві сучасного ритейлу, є дослідження ринку торгівельного обладнання. Аналіз основних тенденцій цього ринку дозволить підприємству визначати попит покупців та швидко пристосовуватися до змін у зовнішньому середовищі.

Проаналізуємо динаміку роздрібного обороту в Україні за останні роки.

Рис. 2.1 Обсяг обороту роздрібної торгівлі в Україні в 2019-2022рр., млн. грн.

Примітка: розроблено автором на основі дослідження

На рис. 2.1 можемо спостерігати, що у період з 2019 р. по 2021р. відбулося значне зростання обсягів реалізації у роздрібній торгівлі на 10 %, а з 2020р. по 2021р. на 19 %. Проте у 2022 році відбувся спад товарообігу близько на 3,4 %

порівняно з попереднім роком. Такі зміни можуть буди поясненні впливом військової агресії росії, а саме постійними ракетними обстрілами великих торгових центрів у різних областях України. За період повномасштабного вторгнення російські ракети зруйнували понад 20 торгових центрів, що завдало непоправних збитків українським ретейлерам.

Сучасне та якісне торгівельне обладнання відіграє важливу роль в збільшенні прибутків компанії. Привабливе торгівельне обладнання створює позитивне враження про торговий простір та підсилює у покупця значення відповідного бренду. На рис. 2.2 можемо побачити структуру замовлень обладнання у різних сферах діяльності.

Рис. 2.2 Структура замовлень торговельного обладнання

Примітка: розроблено автором на основі дослідження

На основі структури замовлень торговельного обладнання можна зробити наступні висновки:

1. Сфера Послуг (40%): Значна частина замовлень спрямована на сферу послуг, що може включати, наприклад, ресторани, кафе, готелі, торгові точки з послугами та інші. Це свідчить про попит на торговельне обладнання для бізнесів, які надають різноманітні послуги.

2. Склади та Логістичні Підприємства (10%): Замовлення від складів та

логістичних підприємств вказують на потребу в спеціалізованому обладнанні для ефективного зберігання та управління логістичними процесами.

3. Промисловість (15%): Значна частина замовлень від промислових підприємств свідчить про те, що торговельне обладнання використовується виробничими компаніями для організації робочих просторів та покращення виробничих процесів.

4. Роздрібна Торгівля (35%): Значна частка замовлень припадає на роздрібну торгівлю, що включає робочі місця, вітрини та інше обладнання для роздрібних магазинів. Це свідчить про активність у сфері роздрібної торгівлі та попит на спеціалізовані рішення для цього сегменту.

Основними виробниками та постачальниками торговельного обладнання в Україні є компанія «Модерн-Експо», «Алюр Плюс», «Торпал».

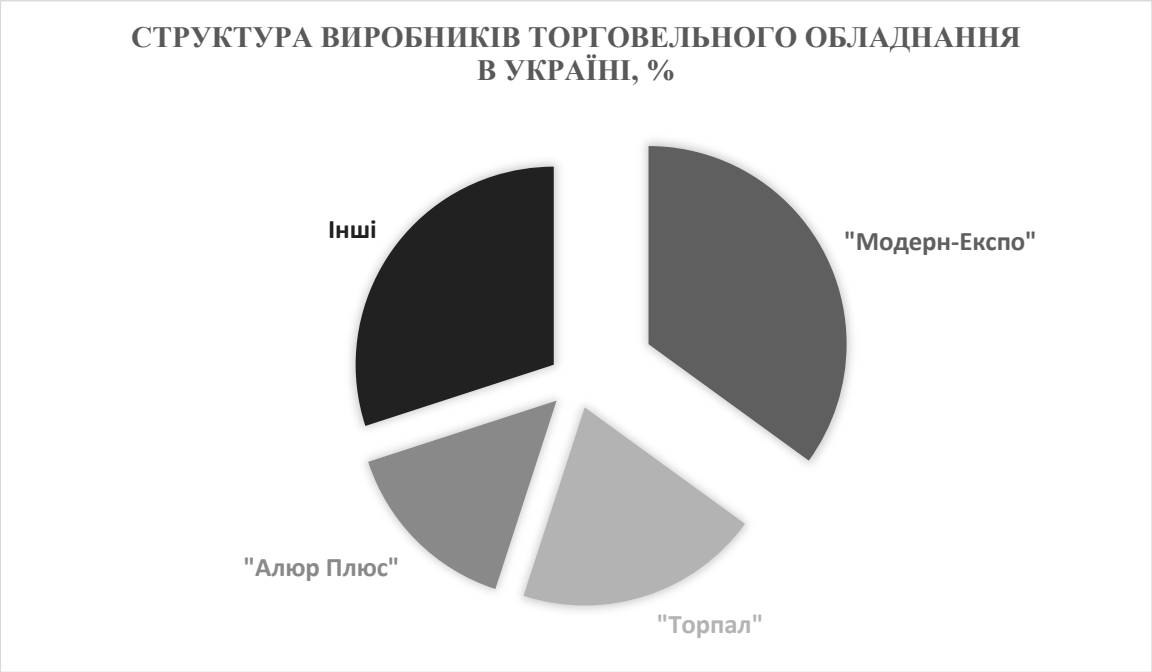

Рис. 2.3 Структура торговельного обладнання в Україні

Примітка: розроблено автором на основі дослідження

Решту ринку займають інші виробники, серед яких компанія «Аском», «ПроКупець», «Торгтехніка», «Торгмебель», «ТД Стандарт», «Екостандарт». Нижче наведе структуру виробників торгівельного обладнання.

Підприємство [redacted] має значну частку ринку торговельного обладнання в Україні, що свідчить про його визнання та довіру серед клієнтів.

Ймовірно, компанія має конкурентні переваги, такі як висока якість продукції, інноваційні рішення або ефективні стратегії маркетингу. За даними журналу Forbes Ukraine [redacted] входить в число 50 найбільших експортерів України у 2022 році.

Для дослідження міжнародного попиту на українське торговельне обладнанням проаналізуємо обсяг експорту українського гарнітуру за даними Української асоціації меблевиків.

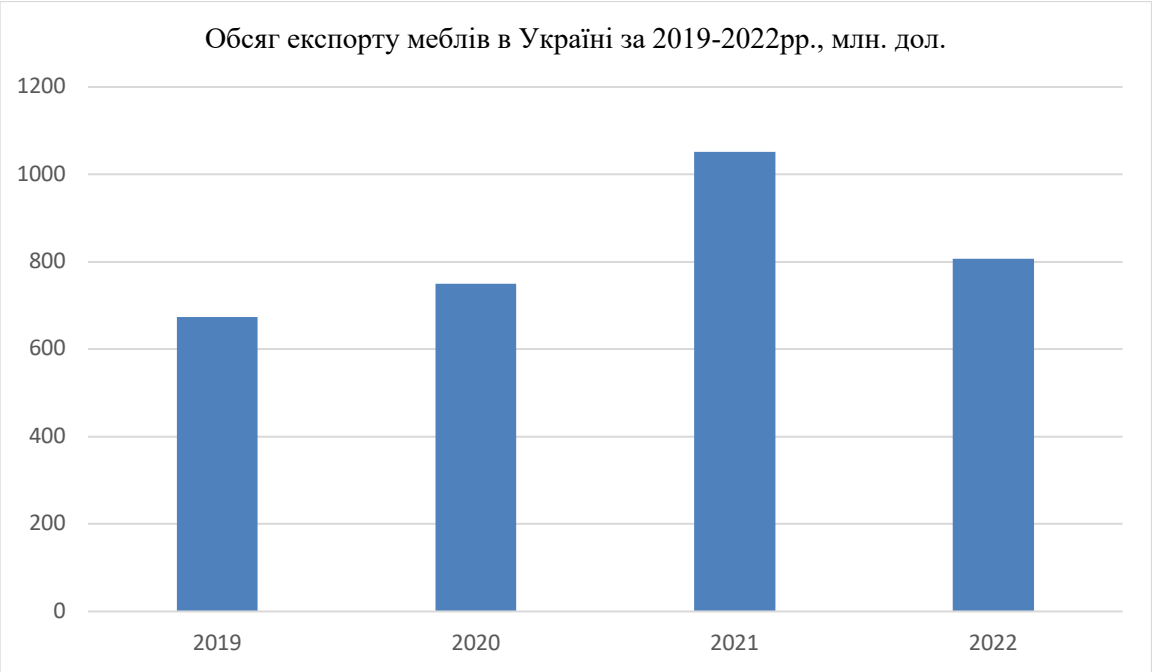

Рис. 2.4 Обсяг експорту меблів в Україні за 2019-2022рр., млн. дол.

Примітка: розроблено автором на основі дослідження

За даними рис. 2.4 можна зробити висновок, що обсяг експорту меблів за 2022 рік зменшився на 23,3 % відповідно до довоєнного 2021 року. Причиною цього стало припинення поставок до країни агресора Російської федерації, а також зменшення обсягів експорту до країн Близького Сходу на 20-40 %. Проте в загальному, незважаючи на нестабільну економічну та політичну ситуацію в країні, українські меблі продовжують користуватися попитом на міжнародному ринку.

У 2022 році українська меблі були експортовані до 99 країн світу, що у свою чергу у 2021 році становило 120 країн. Найбільші країни-імпортери зазначені на рис. 2.5.

Польща є найбільшим імпортером українських меблів, займаючи значну частку - 34,91%. Це може бути пов'язано з ефективними торговельними відносинами, географічною близькістю та попитом на українські меблі.

Німеччина, Данія, Австрія, Бельгія та інші європейські країни також виявляють інтерес до українських меблів. Це може свідчити про високу якість продукції та відповідність європейським стандартам. Республіка Молдова, Велика Британія та інші країни, хоч і займають менші частки, все ще є важливими партнерами для експорту українських меблів.

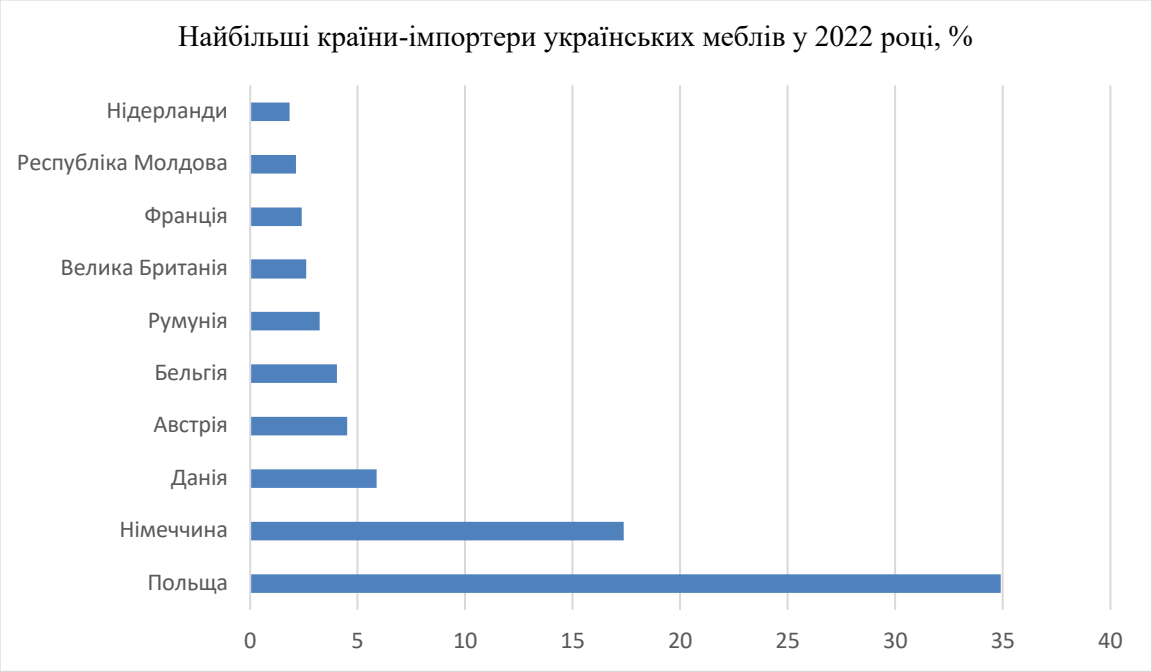

Рис. 2.5 Найбільші країни-імпортери українських меблів у 2022 році, %

Примітка: розроблено автором на основі дослідження

2.2 Економіко-організаційна характеристика XXXXXXXXXXXXXXXXXX

[redacted] підприємство у формі товариства з обмеженою відповідальністю [redacted] – це міжнародна компанія, постачальник комплексних рішень для ритейлу в Центральній і Східній Європі. Виробничі потужності, загальною площею 83 500 кв. м, знаходяться в Луцьку та в Любліні, де знаходиться логістичний центр. Одинадцять офісів компанії знаходяться в Україні, Франції, Польщі, Німеччині, Великобританії, ОАЕ та

інших країнах.

[redacted] постачає обладнання в понад 70 країн світу. В асортименті компанії вже більше 50 тисяч найменувань, а саме: торгові стелажі, касові бокси, обладнання з нержавіючої сталі, каси самообслуговування, стелажі високого складування, POS-обладнання, холодильне обладнання. Сьогодні компанія також розробляє SMART-рішення для ритейлу.

Серед клієнтів [redacted] такі відомі компанії, як: Groupe Auchan, PepsiCo, Metro AG, British American Tobacco, Philip Morris, Imperial Tobacco, Carrefour, ОККО, АТБ, Union COOP, E.Leclerc, Fozzy Group, Rewe Group, Zabka, Henkel, SPAR та інші.

Етапи становлення [redacted] як лідера у виготовленні сучасного обладнання:

1997р. – заснування компанії, яка утворилася шляхом об'єднання української [redacted] та польської компанії [redacted].

1998р. – перший вихід на міжнародний ринок.

2001р. – придбання майнового комплексу у м. Луцьк.

2002р. – започаткували новий напрямок виробництва касових боксів, який представили на виставці EUROSHOP.

2006р. – відкрили напрямок виробництва POP- обладнання.

2007р. – почали масово тиражувати стелажні системи високого складування.

2008р. – вперше в Україні впровадили систему ощадливого виробництва.

2009р. – відкриття у м. Берлін і м. Дубай представництва.

2010р. – новий напрямок виробництва обладнання з нержавіючої сталі.

2012р. – започаткували виробництво холодильного обладнання.

2015р. – відкриття представництв у Парижі та Лондоні, створення міжнародної платформи нетворкінгу – [redacted].

2017р. – розробка «розумного» обладнання для ритейлу.

2018р. – створення бізнес-проекту, що спеціалізується на розробці «розумних» технологій.

2020р. – взяли участь у Euroshop, представивши найбільший та наймаштабніший павільйон на виставці площею 1000 кв.м.

Бізнес – юніти «Модерн- Експо»:

[redacted] – спеціалізується на дизайні ритейл просторів та розробці ритейл концептів. Вони створюють цілісні системи бренду, що включають дизайн-аудит, стратегію, айдентику, бренд-дизайн й розробку дизайн-проєкту інтер'єру та екстер'єру торгового простору.

[redacted] – займається впровадженням комплексних «розумних» розробок та автоматизованих інноваційних рішень, які перетворюють торговельне обладнання на алгоритмізовані та роботизовані системи, а торгові площі – в магазини майбутнього.

[redacted] – спеціалізується на проєктуванні, розробці та виготовленні високотехнологічних рішень для налагодження будь-якого виробництва. Вони займаються автоматизацією ручних виробничих процесів, механообробкою, термообробкою, проєктуванням роллформінгів, форм, штампів, екструдерів та ін.

«Модерн-Експо» керується принципами гнучкості в роботі, комплексного підходу, операційної досконалості і чесних і взаємовигідних комплексів з унікальним дизайном та функціоналом. Головними напрямами діяльності підприємства є: виготовлення стелажів, касових боксів, брендового обладнання, тощо; реалізація продукції як на вітчизняних, так і на зарубіжних ринках; надання комплексу дизайнерських послуг для інтер'єру торгових комплексів.

В компанії переважає лінійно-функціональна організаційна структура із елементами матричної (див. дод. А, Б). Керівництво здійснює генеральний директор та його заступники.

2.3 Аналіз внутрішнього середовища досліджуваного підприємства для відшукання резервів розвитку

Для дослідження та оцінки динаміки фінансового стану ХХХХХХХХХХХХХХХХХХ необхідно здійснити горизонтальний аналіз активів

та пасивів підприємства. Цей аналіз допоможе виявити потенційні ризики та можливості, а також визначити зміни, які позитивно чи негативно впливають на фінансову стійкість підприємства.

Загальна сума активів у 2022 році збільшилася на 856 337 тис. грн. або більш, ніж на 34 %. У 2023 році порівняно з 2022 роком загальна сума активів збільшилася на 574 496 тис. грн. або на 17,05 %. Це збільшення відбулось переважно за рахунок значного збільшення оборотних активів.

Таблиця 2.2

Горизонтальний аналіз активів ХХХХХХХХХХХХХХХХХХ

у 2021-2023 рр., тис. грн.

Показник	2021	2022	2023	Абс. приріст, +,- 2022/2021	Абс. приріст, +,- 2023/2022	Відн. приріст, % 2022/2021	Відн. приріст, % 2023/2022
Основні засоби	932005	1102473	1085301	170468	-17172	18,29	-1,56
НЕОБОРОТНІ АКТИВИ	961969	1168745	1146322	206776	-22423	21,50	-1,92
Запаси	272417	572764	403540	300347	-169224	110,25	-29,55
Дебіторська заборгованість за продукцію, товари, роботи, послуги	935002	1359825	1499362	424823	139537	45,44	10,26
Гроші та їх еквіваленти	252679	155192	816528	-97487	661336	-38,58	426,14
ОБОРОТНІ АКТИВИ	1528810	2195703	2796995	666893	601292	43,62	27,38
АКТИВИ	2512484	3368821	3943317	856337	574496	34,08	17,05

Примітка: розраховано автором на основі даних ХХХХХХХХХХХХХХХХХХ

Абсолютна величина збільшення оборотних активів у 2022 році склала 666 893 тис. грн, у 2023році – 601 292 тис. грн. або більше, ніж 43,62 % і 27,38 % відповідно їх річної величини. У той же час у 2022 році, на 18,29 % збільшилася сума основних засобів підприємства (в абсолютному вимірюванні – на 170 468 тис. грн.) Це відбулось внаслідок купівлі обладнання для модернізації виробництва. Натомість у 2023 році вартість необоротних активів зменшилася на 1,56 %, що може бути спричинена різними факторами такі як знос або продаж обладнання.

Що стосується структури оборотних коштів, то можна зазначити, що вона значно покращилася. Виробничі запаси збільшилися за 2022 рік на 300 347 тис. грн або на 31,43%. Зменшилася також величина грошових кошти на 97 487 тис. грн. за 2022р. Проте зменшення запасів на 29,55 % у 2023 році та збільшення грошей на 426,14 % свідчить про зростання обороту підприємства і позитивні тенденції у його роботі. В той же час у 2022 і 2023 році спостерігається тенденція до збільшилася суми і частки дебіторської заборгованості за товари та послуги — в абсолютному вимірюванні на 24823 тис. грн. і 139537 тис. грн. відповідно. Це означає, що підприємство фактично кредитувало своїх партнерів по бізнесу, які вчасно не розраховувалися за товари та послуги, що надавалися підприємством.

Таблиця 2.3

Горизонтальний аналіз пасивів (джерел фінансування активів)

ХХХХХХХХХХХХХХХХХХ у 2020-2022 рр., тис. грн.

Показник	2021	2022	2023	Абс. приріст, +,- 2022/2021	Абс. приріст, +,- 2023/2022	Відн. приріст, % 2022/2021	Відн. приріст, % 2023/2022
Нерозподілений прибуток (непокритий збиток	1398319	1792102	2377412	393783	585310	28,16	32,66
ВЛАСНИЙ КАПІТАЛ	1487986	2014861	2578049	526875	563188	35,41	27,95
Довгострокові кредити банків	188541	123072	98652	-65469	-24420	-34,72	-19,84
ДОВГОСТРОКОВІ ЗОБОВ'ЯЗАННЯ	259573	219407	189410	-40166	-29997	-15,47	-13,67
Короткострокові кредити банків	244471	337909	513915	93438	176006	38,22	52,09
Поточна кредиторська заборгованість за товари, роботи, послуги	364634	607385	493691	242751	113694	66,57	-18,72
КОРОТКОСТРОКОВІ ЗОБОВ'ЯЗАННЯ	764925	1134553	1175858	369628	41305	48,32	3,64
БАЛАНС	2512484	3368821	3943317	856337	574496	34,08	17,05

Примітка: розраховано автором на основі даних ХХХХХХХХХХХХХХХХХХ

Факт зростання суми власного капіталу вказує на підвищення рівня благополуччя власників. Зростання загальної суми зобов'язань забезпечує більш повне розкриття наявного потенціалу компанії, хоча призводить до підвищення залежності від зовнішніх постачальників фінансових ресурсів.

При аналізі пасивів підприємства слід зазначити, що довгострокові

зобов’язання підприємства за 2022 рік скоротилися на 15,47 % та за 2023 рік на 13,67 %, в свою чергу короткострокові зобов’язання збільшилися на 48,32 % за 2022 рік та на 3,64 % за 2023 рік за рахунок збільшення кредиторської заборгованості та кредитів банку. Динаміка показників ліквідності є негативною за рахунок збільшення короткострокової заборгованості, що зменшує фінансову стійкість.

Для аналізу забезпеченості підприємства основними засобами та їх динаміки проведемо аналіз основних показників.

Таблиця 2.4

Показники забезпеченості ХХХХХХХХХХХХХХХХХХосновними засобами та їх динаміки за 2021-2023рр.

Показник	2021	2023	2023	Абсолютне відхилення, 2023/2021
Показники забезпеченості підприємства основними засобами				
Фондовіддача	2,25	3,9	3,18	0,93
Фондомісткість	0,42	0,25	0,31	-0,11
Частка основних засобів у активах, %	37,10	32,73	27,52	-9,58
Показники оцінки стану і руху основних засобів				
Коефіцієнт зносу основнихзасобів	18,59	3,3	11,68	-6,91
Коефіцієнт придатностіосновних засобів	81,41	96,70	88,33	6,92
Коефіцієнт оновлення основних засобів	0,05	0,15	0,04	-0,01
Коефіцієнт вибуття основних засобів	0,18	0,04	0,12	-0,06

Примітка: розраховано автором на основі даних ХХХХХХХХХХХХХХХХХ

На основі цих показників можна зробити висновок, що зростання фондовіддачі свідчить про ефективність використання основних засобів. Проте зниження фондомісткості на 0,11 у 2023 році порівняно з 2021 роком може вказувати на зменшення витрачання коштів на основні засоби, про що свідчить і низький коефіцієнт оновлення ОЗ. Спостерігається поступове зниження ваги основних засобів у активах підприємства. У 2023 році коефіцієнт зносу становив 11,68, що може вказувати на те, що багато основних засобів перебувають довгий час в експлуатації, проте згідно коефіцієнту придатності машини та обладнання

знаходяться у хорошому стані. Коефіцієнт оновлення та вибуття основних засобів показують, що оновлення основних засобів відбувається на низькому рівні.

Аналіз фінансових результатів підприємства дозволить виявити збільшення або зниження прибутковості та знайти додаткові резерви для зростання обсягів виробництва.

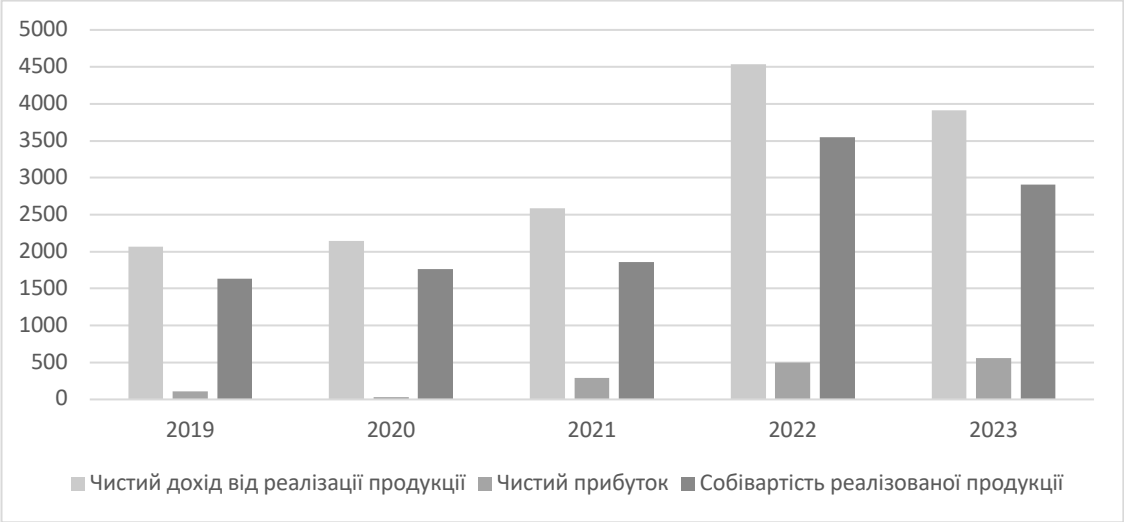

Рис. 2.5. Аналіз фінансових результатів XXXXXXXXXXXXXXXXXX за 2019-2023р.,млн. грн

Як бачимо, протягом аналізованого періоду компанія постійно збільшує обсяги виробництва та реалізації продукції за рахунок чого збільшується чистий дохід. У 2023 році чистий дохід склав 3 916 млн. грн, що на 1 845 млн. грн. більше, ніж 4 роки тому. Одним з важливих показників ефективності діяльності підприємства є рентабельність.

Рентабельність реалізованої продукції з 2021 року зросла з 15,61 % до 19,37 %. Це свідчить про те, що підприємству вдалося підвищити прибутковість своєї діяльності. Зростання рентабельності може бути пов’язано з оптимізацією виробничих процесів, зменшенням собівартості продукції або підвищенням цін на продукцію.

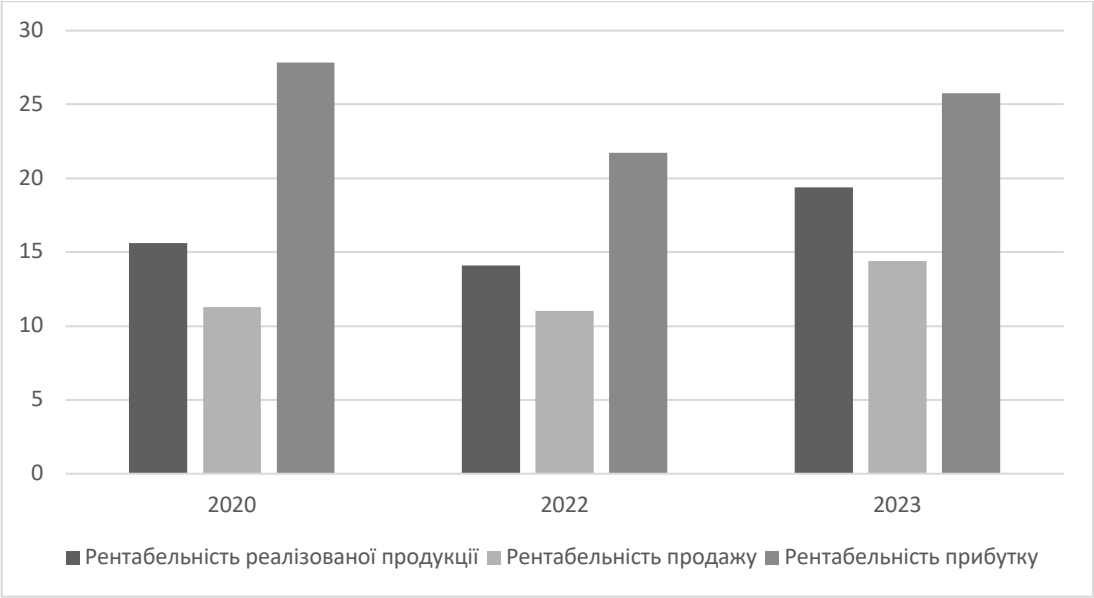

Рис. 2.6 Аналіз рентабельності XXXXXXXXXXXXX за 2021-2023 рр.

Примітка: розраховано автором на основі даних XXXXXXXXXXXXXXXXX

Оскільки за останні роки собівартість продукції становить більше 70 % чистого доходу підприємства, то очевидно, що підприємство використовує метод збільшення продажів, шляхом виходу на нові, а в більшості міжнародні, ринки збуту.

Рентабельність продажів є важливою характеристикою у ціноутворенні продукції. Як бачимо у 2023 році 14,38 % у загальній виручці припадає на прибуток підприємства.

Рентабельність прибутку допомагає визначити прибутковість бізнесу в цілому. З 2021 року рентабельність прибутку зменшилася з 27,85 % до 25,74 %. Такий спад може спричинити збільшення операційних витрат підприємства.

Аналіз витрат є важливою складовою ефективного управління підприємством. Від рівня та динаміки витрат залежать прибутки або збитки суб'єкта господарювання.

Дані таблиці свідчать про тенденцію збільшення як виробничих, так і невиробничих витрат в абсолютному розмірі. Так у 2022 р. собівартість реалізованої продукції збільшилася на 1683792 тис. грн, порівняно з 2021 роком. Проте у 2023 році собівартість зменшилася на 8,61 %, що у свою чергу збільшило прибутковість підприємства.

Таблиця 2.3

Аналіз витрат XXXXXXXXXXXXXXXXXX за 2021-2023 р.

Види витрат	2021		2022 р.		Відхилення від 2021 р.		2023		Відхилення від 2022 р.	
	Сума, тис. грн.	Структура %	Сума, тис. грн.	Структура %	Абсолютне, тис. грн.	Структура %	Сума, тис. грн	Структура %	Абсолютне, тис. грн.	Структура %
Собівартість реалізованої продукції	1863905	74,81	3547697	85,43	1683792	10,63	2908120	76,83	-639577	-8,61
Адміністративні витрати	140115	5,62	169244	4,08	29129	-1,55	217721	5,75	48477	1,68
Витрати на збут	196845	7,90	200302	4,82	3457	-3,08	191542	5,06	-8760	0,24
Інші операційні витрати	62394	2,50	101406	2,44	39012	-0,06	177576	4,69	76170	2,25
Фінансові витрати	25939	1,04	19098	0,46	-6841	-0,58	24498	0,65	5400	0,19
Інші витрати	135890	5,45	525	0,01	-135365	-5,44	139160	3,68	138635	3,66
Податки на прибуток	66511	2,67	114348	2,75	47837	0,08	126659	3,35	12311	0,59
Разом витрат	2491599	100	4152620	100	X	X	3785276	100	X	X

Протягом аналізованого періоду собівартість становить значну частину у структурі витрат, підприємству необхідно оптимізувати процес виробництва та ефективніше управляти запасами. Спостерігається тенденція до збільшення витрат за останні декілька років, що пов’язано з постійним збільшенням обсягів виробництва. Також збільшилися витрати на операційну діяльність підприємства,

тому варто розглянути їхню структуру детальніше.

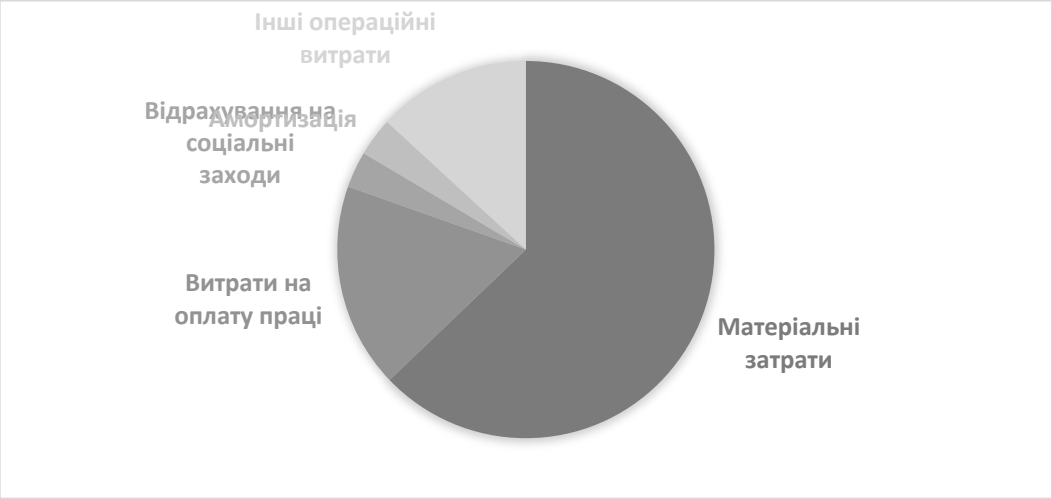

Рис. 2.6 Структура операційних витрат XXXXXXXXXXXXXXXXXX за 2023 р.

Аналіз структури операційних витрат за економічними елементами свідчить, про те, що виробництво обладнання для ритейлу є дуже матеріаломістким. Як бачимо на рис. 2.6 63,85 % сукупних витрат займають матеріальні витрати, тобто придбання матеріалів, сировини, комплектуючих, МШП, які використовуються у виробництві. Значну частину витрат, а саме 17,57 % становить фонд заробітної плати. У 2023 році XXXXXXXXXXXXXXXXX згідно звіту про рух грошових коштів оплата праці становила 463 499 тис. грн., 3,3 % витрат припадає на амортизацію, що цілком зрозуміло, зважаючи на матеріально-технічну базу підприємства. 3,11 % та 13,17 % витрат становлять відрахування на соціальні заходи та інші операційні витрати відповідно.

Станом на кінець 2023 року середня чисельність працівників склала 1790 осіб. У гендерній структурі працівників 78 % становлять чоловіки, решту 22 % жінки. Для навчання та підвищення кваліфікації працівників було впроваджено проект корпоративного університету – «Модерн-Академія». На рис. 2.7 можемо побачити, що найбільше працівників, а саме 42,32 % з професійно-технічної освітою, 26,91 % з повною загальною та 18,15 % з повною вищою. Найменше працівників з базовою загальною середньою освітою – 12,63 %, що ще раз доводить факт, що компанія значну увагу приділяє кваліфікації працівників.

Вільні обігові кошти можуть стати джерелом фінансуванні формування системи захистку цифрових даних в обліку і оподаткування. На рис. 2.3 наведено

структуру руху коштів ХХХХХХХХХХХХХХХХХХ.

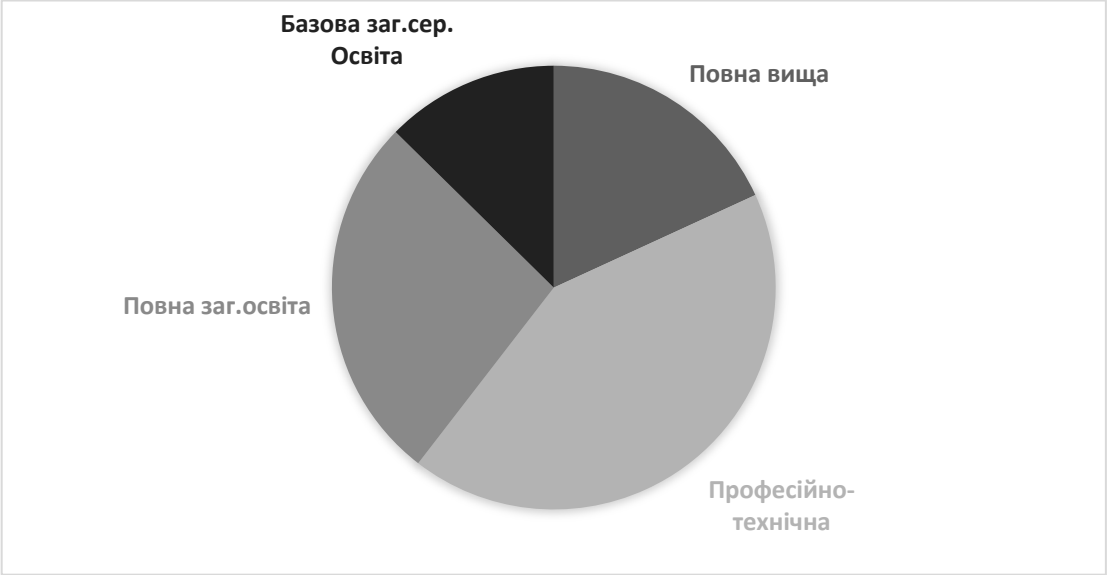

Рис. 2.7 Структура працівників за видом освіти за 2023 рік.

Чистий рух обігових коштів від операційної діяльності 620 420 тис. грн., можна зробити висновок про наявність резервного капіталу, який можна використати для здійсненні інноваційної діяльності. Крім того, оскільки значну частину витрачання коштів становлять податки, то оптимізація цих витрат допоможе вивільнити додаткові кошти.

Проаналізуємо основні показники власних обігових коштів ХХХХХХХХХХХХХХХХХХ за 2023 рік:

1) Величина власних оборотних коштів:

ВОК = ОА-ПЗ = 2 796 995 - 1 175 858 = 1 621 137 тис. грн

ОА – оборотні активи, ПЗ – поточні зобов’язання.

Отже, після розрахунків зі всіма поточними зобов’язаннями у розпорядження підприємства залишається 1 621 137 тис. грн.

2) Ступінь забезпеченості поточної діяльності власними оборотними коштами:

$$К_з = \frac{ВОК}{ОА} = \frac{1621137}{2796995} = 0{,}58.$$

Мінімальне значення показника – 0,1. Коефіцієнт забезпеченості оборотними коштами у ХХХХХХХХХХХХХХХХХХ - 0,58, що свідчить про

стабільний фінансовий стан та платоспроможність. 58 % поточних зобов'язань покриваються власними оборотними коштами.

3) Маневреність власних оборотних коштів:

$$K_м = \frac{ГК}{ВОК} = \frac{816528}{1621137} = 0{,}5, \text{ де ГК – грошові кошти}$$

Коефіцієнт маневреності 0,5 вказує на середню здатність підприємства використовувати власні кошти для фінансування додаткових проектів.

4) Частка власних обігових коштів у покритті запасів:

$$К_{п.з} = \frac{ВОК}{З} = \frac{1621137}{278483} = 5{,}8, \text{ де З – запаси}$$

Найнижча межа цього показника 50 %, у підприємства цей показник становить 58 %, що означає, що покриття запасів здійснюється в основному за рахунок внутрішніх джерел. У цілому це позитивний показник, що ще раз доводить фінансову стійкість підприємства.

Узагальнивши всі показники, можна зробити висновок, що XXXXXXXXXXXXXXXXXX має достатньо вільних обігових коштів для розвитку та здійснення інноваційної діяльності.

Для забезпечення фінансування інноваційний проектів важливо також проаналізувати ліквідність активів, тобто оцінити платоспроможність підприємства у разі виникнення форс-мажорних ситуацій.

Таблиця 2.4

Розрахунок показників ліквідності за 2021-2023рр. XXXXXXXXXXXXXXXXXX

Показник	2021	2022	2023	Відносне відхилення (2023/2021)	Формула розрахунку	Нормативне значення
Коефіцієнт загальної ліквідності ($К_{зл}$)	2,0	1,93	2,38	0,38	$К_{зл} = \frac{\text{Оборотні активи}}{\text{Поточні зобов'язання}}$	>1
Коефіцієнт швидкої ліквідності ($К_{шл}$)	1,44	1,43	1,8	0,36	$К_{шл} = \frac{\text{Об. активи} - \text{Запаси}}{\text{Поточні зобов'язання}}$	> 0,8
Коефіцієнт абсолютної ліквідності ($К_{ал}$)	0,33	0,14	0,69	0,36	$К_{ал} = \frac{\text{Грошові кошти}}{\text{Поточні зобов'язання}}$	> 0,2

Загалом спостерігається зростання усіх показників з року в рік. Збільшення коефіцієнту загальної ліквідності на 0,38 за два роки свідчить по те, що керівництво підприємства покладає значні зусилля для покращення фінансової

стабільності компанії. Коефіцієнт швидкої ліквідності та абсолютної ліквідності також збільшився на 0,36, це може означати покращення здатності підприємства задовольняти свої поточні зобов'язання за рахунок найбільше ліквідних активів. Можна зробити висновок, що у разі непередбачуваних витрат, підприємство зможе здійснювати свою операційну діяльність без значного впливу на зменшення прибутковості компанії.

Для виявлення потенційних можливостей та процесів, які можливо слабо функціонують необхідно провести аналіз показників ділової активності ХХХХХХХХХХХХХХХХХ. Цей аналіз допоможе спланувати діяльність підприємства і з прогнозувати можливі фінансові результати.

Таблиця 2.5

Розрахунок показників ділової активності ХХХХХХХХХХХХХХХХХ за 2023 р.

Показник	Формула	2023
Коефіцієнт оборотності активів (Коа)	$К_{оа} = \frac{\text{Виручка від реалізації}}{\text{Середня вартість активів}}$	0,99
Тривалість одного обороту активів (Та)	$Т_{а} = \frac{\text{К – сть днів у періоді}}{\text{Коа}}$	368,6
Коефіцієнт оборотності необоротних активів (Кона)	$К_{она} = \frac{\text{Виручка від реалізації}}{\text{Середня варт. необ. активів}}$	3,41
Тривалість одного обороту необоротних активів (Тна)	$Т_{на} = \frac{\text{К – сть днів у періоді}}{\text{Кона}}$	107,03
Коефіцієнт оборотності оборотних активів (Кооа)	$К_{ооа} = \frac{\text{Виручка від реалізації}}{\text{Середня варт. оборт. активів}}$	1,4
Тривалість одного обороту оборотних активів (Тоа)	$Т_{оа} = \frac{\text{К – сть днів у періоді}}{\text{Кооа}}$	260,71
Коефіцієнт оборотності запасів (Коз)	$К_{оз} = \frac{\text{Виручка від реалізації}}{\text{Середня варт. запасів}}$	9,7
Тривалість одного обороту запасів (Тз)	$Т_{з} = \frac{\text{К – сть днів у періоді}}{\text{Коз}}$	37,63
Коефіцієнт оборотності дебіторської заборгованості	$К_{одз} = \frac{\text{Виручка від реалізації}}{\text{Середня варт. дебітор. забрг.}}$	2,61
Тривалість одного обороту дебіторської забогованості	$Т_{дз} = \frac{\text{К – сть днів у періоді}}{\text{Кодз}}$	139,84
Коефіцієнт оборотності власного капіталу (Ковк)	$К_{овк} = \frac{\text{Виручка від реалізації}}{\text{Середня варт. власного капіт.}}$	1,52
Тривалість одного обороту власного капіталу (Твк)	$Т_{вк} = \frac{\text{К – сть днів у періоді}}{\text{Ковк}}$	240,13
Коефіцієнт оборотності кредиторської заборгованості	$К_{окз} = \frac{\text{Виручка від реалізації}}{\text{Середня варт. кредиторс. заборг.}}$	3,33
Тривалість одного обороту кредиторської заборгованості	$Т_{кз} = \frac{\text{К – сть днів у періоді}}{\text{Кокз}}$	109,60

Проаналізуємо детальніше показники ділової активності:

1. Коефіцієнт оборотності активів (Коа): 0,99

Цей показник показує, що активи обертаються приблизно один раз на рік. Тобто, підприємство витрачає близько 368,6 днів, щоб здійснити повний оборот активів. Причинами такого довгого обороту можуть бути великі запаси матеріалів, довгий період реалізації товару або неефективне управління активами.

2. Коефіцієнт оборотності необоротних активів (Кона): 3,41

Цей показник показує, що необоротні активи обертаються досить швидко, що підтверджує ефективне використання основних засобів та обладнання.

3. Коефіцієнт оборотності оборотних активів (Кооа): 1,4

Цей показник вказує на те, що оборотні активи обертаються дещо повільніше, ніж загальні активи. Тривалість одного обороту оборотних активів становить 260,71 день. Потрібно покращити цей показник.

4. Коефіцієнт оборотності запасів (Коз): 9,7

Високий показник Коз свідчить про те, що запаси дуже швидко обертаються. Це може бути позитивним сигналом для оптимізації запасів та зменшення їхньої вартості. Тривалість одного обороту запасів становить 37,63 дні.

5. Коефіцієнт оборотності дебіторської заборгованості (Кодз): 2,61

Цей показник вказує на те, що дебіторська заборгованість обертається приблизно 2,61 рази на рік. Тривалість одного обороту дебіторської заборгованості складає 139,84 дні. Підприємству необхідно зменшити час на оплату від клієнтів.

6. Коефіцієнт оборотності власного капіталу (Ковк): 1,52

Цей показник вказує на те, що власний капітал обертається приблизно 1,52 рази на рік. Тривалість одного обороту власного капіталу становить 240,13 дні.

7. Коефіцієнт оборотності кредиторської заборгованості (Кокз): 3,33

Цей показник вказує на те, що кредиторська заборгованість обертається приблизно 3,33 рази на рік. Тривалість одного обороту кредиторської заборгованості складає 109,60 дні. Висока оборотність кредиторської заборгованості може свідчити про добре управління обов’язками перед кредиторами.

Отже, можна зробити висновок, що різні категорії активів та капіталу

обертаються з різною швидкістю. Необхідно збалансувати ці показники, забезпечити ефективне використання ресурсів та покращення фінансової стійкості підприємства.

Для здійснення безпечної діяльності необхідно проаналізувати всі загрози, потенційні проблеми та можливості, що можуть виникнути. SWOT-аналіз дозволить виявити всі фактори, що впливають на підприємство та розробити стратегію розвитку на майбутнє (див. дод. В).

На основі даного SWOT-аналізу можна розглянути наступні стратегії розвитку XXXXXXXXXXXXXXXXX:

1. Використання сильних сторін (Strengths): продовжувати активно розробляти та випускати інноваційні продукти, які відповідають попиту на ринку; розвивати і підтримувати добре функціонуючий веб-сайт та соціальні медіа для привертання нових клієнтів.

2. Подолання слабких сторін (Weaknesses): інвестувати в навчання і розвиток кадрів, щоб заповнити брак висококваліфікованих працівників; розглянути можливості отримання додаткового фінансування або інвестицій для покращення фінансових ресурсів.

3. Використання можливостей (Opportunities): розглянути розширення асортименту продукції, зосереджуючись на інноваціях та вимогах клієнтів: активно залучати інвесторів для підтримки нових проектів та розвитку.

4. Подолання загроз (Threats): розробити плани кризового управління та диверсифікації ризиків для зменшення негативного впливу політичних становищ; шукати нові джерела сировини та матеріалів, щоб зменшити вплив змін цін на них. Оцінка зовнішнього середовища, а саме впливу політичних, економічних, соціальних та технологічних чинників на підприємство, допоможе зменшити ризики та втрати або розробити стратегію для подолання кризових ситуацій у майбутньому (див. дод. Д).

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ЦИФРОВОЇ ІНФОРМАЦІЇ В ОБЛІКУ І ОПОДАТКУВАННІ

3.1 Методичні підходи до оцінки безпеки підприємства

Існує кілька основних методів оцінки рівня економічної безпеки підприємства. Кожен із них має свої особливості, переваги та недоліки, що впливають на практичність їхнього використання в умовах сучасного бізнес-середовища. Розглянемо детальніше найпоширеніші методи оцінки, серед яких: індикаторний, тримірний, ресурсно-функціональний, прибутково-інвестиційний та інші.

1. Індикаторний метод. Цей підхід базується на використанні певних індикаторів – кількісних і якісних показників, що характеризують граничні значення параметрів діяльності підприємства. Недотримання цих значень свідчить про погіршення стану економічної безпеки.

Процес оцінки включає: порівняння фактичних показників із встановленими індикаторами; визначення відхилень та аналіз їхнього впливу на загальний рівень безпеки.

Основна проблема методу – відсутність універсальної методичної бази для формування системи індикаторів, адаптованої до специфіки кожного підприємства. Крім того, складність полягає у визначенні критичних значень індикаторів, що мають враховувати галузеві особливості.

2. Ресурсно-функціональний метод. Цей підхід є одним із найбільш визнаних. Він передбачає оцінку ефективності використання ресурсів підприємства за кожною функціональною складовою економічної безпеки.

Методика включає: розрахунок функціональних критеріїв, які характеризують ефективність нейтралізації негативних впливів і витрати на їх подолання; визначення питомої ваги кожного критерію та формування сукупного показника.

Цей метод дозволяє детально оцінити, наскільки оптимально підприємство використовує свої ресурси для досягнення цілей і мінімізації ризиків. Проте складність застосування полягає у необхідності наявності точних даних щодо витрат і заподіяної шкоди.

3. Прибутково-інвестиційний метод. Основою цього підходу є аналіз чистого прибутку підприємства як головного критерію його економічної безпеки.

Методика включає: визначення обсягу прибутку, доступного для інвестування; співвідношення цього обсягу з необхідними коштами для забезпечення економічної безпеки.

- Наявність стабільного чистого прибутку свідчить про достатній рівень економічної безпеки. Проте цей метод має обмеження: він не враховує можливості оцінки збиткових підприємств, що обмежує його застосування.

4. Тримірний метод. Цей підхід базується на оцінці трьох рівнів економічної безпеки підприємства:

- Поточної – аналіз фінансових показників, ліквідності активів, виконання зобов'язань.
- Тактичної – оцінка ефективності використання ресурсів підприємства.
- Стратегічної – вивчення економічного потенціалу підприємства та його відповідності довгостроковим цілям.

Методика дозволяє комплексно оцінити загальний рівень безпеки залежно від часових горизонтів. Однак його складність полягає у визначенні та інтеграції показників усіх трьох складових.

5. Метод узагальненого показника. Цей підхід передбачає формування єдиного комплексного показника, який синтезує вплив усіх факторів.

Кожна складова безпеки оцінюється на основі системи аналітичних показників.

Комплексні показники інтегруються в один загальний індекс, що відображає досягнутий рівень безпеки.

Метод є зручним для інтерпретації результатів, оскільки дозволяє отримати одне кількісне значення. Однак він потребує ретельного підбору аналітичних показників.

6. Методи прогнозування фінансової неспроможності. До цієї групи належать як кількісні, так і якісні підходи:

- Кількісні моделі (модель Альтмана, шкала Бівера, формула Du Pont) використовують факторний аналіз і розрахунки для оцінки ймовірності банкрутства.
- Якісні методи (метод Ковальова, методика ERNST&WHINNEY) базуються на експертних оцінках, що враховують суб'єктивні аспекти діяльності підприємства.
- Хоча ці підходи широко використовуються у світовій практиці, в Україні вони обмежені через труднощі адаптації до реалій локального ринку.

Кожен із методів оцінки економічної безпеки підприємства має свої переваги і недоліки, тому їх вибір залежить від специфіки діяльності підприємства, доступності даних та поставлених цілей. Використання комплексного підходу, що поєднує кілька методів, дозволяє отримати найбільш точну і надійну оцінку рівня безпеки підприємства [13].

3.2 Методичні рекомендації що створення системи безпеки цифрових даних в обліку і оподаткування за допомогою диджитал-технологій

Важливо розуміти, що цифрова безпека – це процес. Постійно виникають про нові загрози, що вимагають освоєння та застосування нових інструментів, які з'являються.

Можна виокремити основні правила цифрової безпеки, що можуть стати основою методичних рекомендацій.

1. Використовувати ліцензійне програмне забезпечення, зокрема на телефонах і планшетах, робочих та домашніх комп'ютерах.
2. Регулярно оновлюати все програмне забезпечення.
3. Встановлювати антивірусні програми та firewall (міжмережевий екран, фаєрвол). Антивірус вирішує проблему зараження вірусами, а фаєрвол відслідковує міжмережеві зв'язки комп'ютера та мережі Інтернет і, відповідно,

допомагає захищатись від загроз ззовні. У Windows, то можна використовувати вбудовані захисні програми Windows Defender або ж якісь інші – все залежить від того, кому ви довіряєте.

4. Встановлювати пароль на вхід у пристрій (телефон, планшет, комп'ютер). Складний унікальний пароль – це такий, котрий містить великі літери, маленькі літери, спеціальні символи, і розмір його загалом не менше 14 символів – це мінімальний стандарт, а ще краще 20 чи 30. Унікальність – це означає, що кожен обліковий запис повинен мати власний пароль.

5. Використовуйте менеджер паролів. LastPass – це онлайн менеджер паролів для тих облікових записів, які ви створюєте онлайн. KeePass – це офлайн менеджер, де ви самостійно забезпечуєте безпеку паролів.

6. Не використовуйте ненадійні поштові сервіси, соціальні мережі, месенджери. Ненадійні сервіси – це ті, які надавали інформацію про своїх користувачів, або ж вони поганої якості, тобто не використовують шифрування, або були скомпрометовані.

7. Розділяйте облікові записи.

Наприклад, у нас є поштові скриньки окремо для роботи і для дому. Якщо зламали нашу домашню скриньку, то не отримали доступ до робочої, і навпаки. Навіть, якщо ми комунікацію розділяємо між різними месенджерами: наприклад, частина переписки в WhatsApp, а частина в Viber – це вже захищає інформацію, тому що тим, хто атакує, треба отримати доступ до ще одного каналу комунікації.

8. Блокувати пристрої у перервах та після закінчення роботи.

Для Windows – це блокування клавішами Win+L, в Mac комп'ютерах ви просто блокуєте кришку, і він переходить в режим сну та запитує пароль.

9. Використовуйте повнодискове шифрування пристроїв.

Якщо ви користуєтесь останніми моделями iPhone або телефонами преміум-класу з системою Android, то таке шифрування відбувається за замовчуванням.

10. Видаляти історію з браузера та кеш. Наприклад, CCleaner – це програма, за допомогою якої можна видаляти такі тимчасові файли.

11. Не зазначати очевидні відповіді для відновлення доступу до свого облікового запису.

12. Не використовуйте для відновлення доступу незахищені поштові скриньки. Якщо у вас є добре захищена поштова скринька на Gmail, а інша скринька на Mail.ru, і вони пов’язані між собою функцією відновлення, тоді потенційно ви є вразливими.

13. Користуйтесь секретними месенджерами, якщо вирішили вести таємну переписку. Наприклад, Viber, Signal, таємні чати в Telegram.

14. Використовуйте месенджери з шифруванням від пристрою до пристрою – Signal, WhatApp, Viber, а в Telegram - секретний чат. В такому випадку у сервіс-провайдера немає можливості читати вашу переписку.

15. Не клікайте на підозрілі посилання.

16. Не ловіться на фішинг. Фішинг – вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів.

17. Робіть резервні копії важливих файлів в хмарних сховищах. Хмарні сховища – це Google Диск, Dropbox. Статистично є дуже ймовірним, що може трапитись пошкодження жорсткого диску або флешки без можливості відновлення.

18. Робіть двофакторну авторизацію для важливих облікових записів.

Facebook, Dropbox, Microsoft, Yandex Диск, ВКонтакте, Gmail – скрізь, де це можливо, краще застосовувати двофакторну авторизацію. Це означає, що, окрім паролю, який ви знаєте, вам потрібно зазначити другий фактор – це може бути або СМС-повідомлення, або локально згенерований код на вашому телефоні через Google автентифікатор.

19. Використовуйте технології VPN (Virtual Private Network – віртуальна приватна мережа) при підключенні до публічного Wi-Fi. VPN – це тунель від вашого ПК до іншого комп’ютера, а потім до мережі Інтернет.

20. Використовуйте мережу Tor, якщо хочете бути анонімними. Tor (The Onion Router) – це інструмент анонімності, а VPN – інструмент безпеки.

21. Змінюйте дефолтний пароль на домашньому Wi-Fi-роутері. Дефолтні паролі – це паролі за замовчуванням. Ваш роутер підключений до мережі

Інтернет. Якщо на ньому стандартні паролі, як от «admin» або номер вашого телефону, то до нього може підключитись зловмисник.

Три принципи інформаційної безпеки: конфіденційність, цілісність і доступність – це запорука ефективного захисту даних та безпеки інфраструктури організації. Ці три поняття – основоположні принципи для впровадження плану InfoSec.

3.3 Інструменти для захисту даних

Бухгалтерські системи можуть бути вразливими до різноманітних кіберзагроз. Можна виокремити основні проблеми:

Витік даних. Один із найбільших ризиків, пов’язаний із бухгалтерськими системами, полягає в тому, що зловмисники можуть отримати доступ до фінансової інформації, такої як баланси, звіти, інформація про операції. Це може статися через слабкі місця в системах безпеки або через несанкціонований доступ до баз даних.

Атаки на програмне забезпечення. Зловмисники можуть скористатися уразливими місцями в програмному забезпеченні бухгалтерської системи (наприклад, уразливості в протоколах обміну даними або в алгоритмах шифрування) для того, щоб здійснити атаку. Атаки можуть включати злочинний доступ до даних або їх пошкодження.

Фішинг та соціальна інженерія. Зловмисники можуть використовувати методи соціальної інженерії для того, щоб отримати доступ до облікових даних працівників підприємства, шляхом обману. Наприклад, фішинг-атаки, коли зловмисники створюють фальшиві електронні листи або вебсайти, які імітують справжні, щоб отримати логіни, паролі чи іншу конфіденційну інформацію.

Шкідливе програмне забезпечення. Включаючи віруси, трояни, руткіти та програмне забезпечення для викрадення даних. Шкідливі програми можуть проникати в бухгалтерські системи через заражені файли, посилання чи електронні листи, а потім виводити або змінювати інформацію в облікових базах

даних.

Для забезпечення високого рівня безпеки бухгалтерських систем необхідно використовувати багатошаровий підхід, що включає технічні, організаційні та управлінські заходи захисту.

Шифрування є одним з найефективніших способів захисту даних від несанкціонованого доступу. Всі чутливі фінансові дані, що передаються по мережі або зберігаються на сервері, повинні бути зашифровані за допомогою стандартів шифрування, таких як AES (Advanced Encryption Standard) або RSA. Це забезпечує, що навіть якщо хакер отримає доступ до даних, він не зможе їх прочитати без відповідного ключа.

Приклад: для захисту даних при передачі через Інтернет використовується протокол HTTPS, який забезпечує шифрування всіх даних між клієнтом і сервером, що важливо для забезпечення безпеки в бухгалтерських системах, де дані постійно передаються між користувачами, серверами та іншими підсистемами.

Аутентифікація і доступ. Всі користувачі бухгалтерських систем повинні мати чітко визначені ролі та доступ до конкретної інформації залежно від їхніх прав. Один із найважливіших методів захисту – це двофакторна аутентифікація (2FA), що додає додатковий рівень захисту при вході в систему. Крім традиційного пароля, користувачеві потрібно ввести код, що надсилається на його мобільний телефон або генерується спеціальним додатком.

Приклад: застосування систем, які потребують введення одноразового пароля (OTP) разом із звичайним паролем при вході в бухгалтерську систему. Це значно ускладнює злом пароля за допомогою крадіжки даних або методів соціальної інженерії.

Моніторинг і виявлення вторгнень. Системи для виявлення вторгнень (IDS) є важливою частиною кіберзахисту бухгалтерських систем. Ці системи постійно відстежують трафік і поведінку користувачів, виявляючи аномальні дії або спроби несанкціонованого доступу. Коли відбувається спроба атаки, система має змогу швидко сповістити адміністраторів для вжиття відповідних заходів.

Приклад: використання таких рішень, як Snort або Suricata, для виявлення та

попередження атак на бухгалтерські системи. Вони можуть бути інтегровані з іншими компонентами системи безпеки для автоматичного блокування загроз.

Антивірусне програмне забезпечення та фільтрація трафіку. Спеціальні системи фільтрації трафіку можуть допомогти виявляти шкідливі програми та блокувати їх ще до того, як вони потраплять до системи.

Приклад: програми типу Kaspersky, McAfee, або Bitdefender можуть бути інтегровані з бухгалтерським програмним забезпеченням для автоматичного сканування файлів і електронних листів на наявність шкідливих компонентів.

Оновлення та патч-менеджмент. Регулярні оновлення програмного забезпечення є ключовим моментом для збереження безпеки бухгалтерських систем. Розробники постійно випускають патчі для усунення уразливостей, які можуть бути використані хакерами. Необхідно, щоб програмне забезпечення та операційні системи бухгалтерських систем завжди були актуальними та відповідали останнім стандартам безпеки.

Приклад: автоматизовані системи оновлення, такі як Windows Update або patch management в програмному забезпеченні для бухгалтерії, можуть забезпечити своєчасне оновлення та виправлення вразливостей, зокрема тих, що стосуються захисту від кіберзагроз.

Кіберзахист бухгалтерських систем є важливою складовою інформаційної безпеки підприємства. Використання багатошарових методів захисту, таких як шифрування, аутентифікація, моніторинг систем, антивірусні рішення та регулярне оновлення програмного забезпечення, дозволяє захистити чутливі фінансові дані від загроз, зберігаючи їх цілісність, конфіденційність і доступність. В умовах постійного зростання кіберзагроз підприємствам необхідно постійно вдосконалювати свою стратегію кіберзахисту для збереження своїх даних.

Інструмент: Splunk / SolarWinds / Nagios – системи моніторингу та аналізу логів для відстеження дій користувачів, включаючи спроби несанкціонованого доступу та аномальну активність.

Можливість створення звітів та сповіщень в реальному часі для оперативної реакції на інциденти.

Інструмент для аудиту: OSSEC – відкрита система для моніторингу та

аналізу безпеки [39].

Інструментами антивірусного захисту та захисту від шкідливих програм можна вважати, такі як: Kaspersky Endpoint Security / Bitdefender / Symantec Endpoint Protection – антивірусне програмне забезпечення для захисту робочих станцій та серверів.

Основними інструментами захисту даних можна вважати.

1. Управління доступом та автентифікаціяю Інструмент: Microsoft Active Directory (AD) / LDAP – централізоване управління користувачами та їх правами доступу. Налаштування обмежень доступу на основі ролей (RBAC), керування паролями та їх складністю, моніторинг спроб несанкціонованого доступу.

Додатково: Multi-Factor Authentication (MFA) – двофакторна автентифікація через SMS, мобільний додаток або біометричні дані [36].

2. Шифрування даних. Інструмент: VeraCrypt / BitLocker / PGP (Pretty Good Privacy) – шифрування файлів і дисків для захисту даних у випадку втрати пристрою. Шифрування даних на серверах та в хмарі за допомогою алгоритму AES-256. Протоколи: SSL/TLS для шифрування даних під час передачі через інтернет [37].

3. Резервне копіювання та відновлення даних. Інструмент: Veeam Backup & Replication / Acronis Backup / Commvault- регулярні автоматизовані бекапи даних із можливістю відновлення при збоях. Захист резервних копій з використанням шифрування та зберігання на окремих носіях (наприклад, хмарні сервіси) [38].

4. Моніторинг та аудит. З огляду на те, що бухгалтерські системи містять чутливу фінансову інформацію підприємства, кіберзахист є критично важливим елементом їх функціонування. Атаки на бухгалтерські системи можуть призвести до значних фінансових втрат, викрадення даних або навіть знищення інформації, що робить важливим розуміння проблем безпеки і впровадження ефективних методів захисту.

ВИСНОВКИ

Дослідження основ економічної безпеки підприємства, системи забезпечення цієї безпеки та правових аспектів захисту даних є важливими для ефективного функціонування бізнесу в умовах сучасних загроз та викликів. Важливими аспектами економічної безпеки є як її теоретичні основи, так і практичне застосування принципів і методів захисту, що дозволяють зберігати стабільність та конкурентоспроможність підприємства.

Визначено важливість задоволення інтересів підприємства для забезпечення його економічної безпеки, а також проаналізовані негативні чинники, що можуть впливати на її стабільність.

Акцентовано увагу на системі економічної безпеки підприємства, її меті, завданнях та порядку формування. Правильне формування системи безпеки дозволяє знижувати ризики та загрози, які виникають у процесі діяльності підприємства.

У результаті аналізу фінансово-економічного стану підприємства виявлено високий рівень платоспроможності, що забезпечить формування резервів задля удосконалення системи захисту обліково-аналітичних даних підприємства.

Аналіз фінансово-економічної діяльності XXXXXXXXXXXXX дозволив підтвердити високе положення компанії на ринку за обсягами реалізованої продукції та прибутку. Протягом аналізованого періоду компанія постійно збільшує обсяги виробництва та реалізації продукції за рахунок чого збільшується чистий дохід. У 2022 році чистий дохід склав 3 916 млн. грн, що на 1 845 млн. грн. більше, ніж 4 роки тому. Чистий рух обігових коштів від операційної діяльності 620 420 тис. грн., можна зробити висновок про наявність резервного капіталу, який можна використати для здійсненні інноваційної діяльності.

Рентабельність реалізованої продукції з 2020 року зросла з 15,61 % до 19,37 % у 2022 році. Підприємству вдалося підвищити прибутковість своєї діяльності.

Зростання рентабельності може бути пов’язано з оптимізацією виробничих процесів, зменшенням собівартості продукції або підвищенням цін на продукцію. Оскільки за останні роки собівартість продукції становить більше 70 % чистого доходу підприємства, то очевидно, що підприємство використовує метод збільшення продажів, шляхом виходу на нові, а в більшості міжнародні, ринки збуту.

За допомогою SWOT та PEST- аналізу XXXXXXXXXXXXXXXXXX виявлено зовнішні фактори впливу на підприємство та запропоновано стратегії подолання цих факторів.

Загалом, проведене дослідження підкреслює важливість інтеграції економічної безпеки підприємства з правовими та технологічними аспектами, що забезпечують захист даних на всіх рівнях його діяльності. Врахування всіх цих факторів є необхідним для досягнення стійкості підприємства на ринку та забезпечення його довгострокового розвитку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бенько М. М. Обліково-аналітичне забезпечення економічної безпеки підприємства : підручник. Київ : В-во Ліра-К, 2021. 560 с.

2. Гнилицька Л. В. Обліково-аналітичне забезпечення функціонування системи економічної безпеки підприємства : автореф. дис. на здобуття наук. ступеня д-ра екон. наук : 08.00.09, 21.04.02. Київ, 2013. 35 с.

3. Гнилицька Л. В. Обліково-аналітичне забезпечення економічної безпеки підприємства : монографія. Київ : КНЕУ, 2022. 305 с.

4. Гнилицька Л. В. Обліково-аналітичне забезпечення функціонування системи економічної безпеки суб'єктів господарювання як об'єкт наукових досліджень. Зб. наук. праць «Управління проектами та розвиток виробництва» : Луганськ: Вид. СНУ імені В. Даля, 2021. № 1(37). С. 142–150.

5. Ліпич Л. Г., Хілуха О. А., Кушнір М. А., Скорук О. В. Стратегія управління безпекою підприємства в контексті галузевих загроз. Економічний часопис Східноєвропейського національного університету імені Лесі Українки. 2018. Том 4 №16. С. 41–49.

6. Обліково-аналітичне забезпечення управління економічною безпекою піприємства : монографія / за заг. ред. А. М. Штангрета. Львів : Укр. акад. друкарства, 2017. 276 с.

7. Національне положення (стандарт) бухгалтерського обліку 19 «Об'єднання підприємств», затверджене наказом Міністерства фінансів України від 07.07.1999 р. № 163. URL: https://zakon.rada.gov.ua/laws/show/996-14 (дата звернення: 25.11.2024).

8. Про бухгалтерський облік та фінансову звітність в Україні : Закон України від 16.07.1999 № 996. URL: https://zakon.rada.gov.ua/laws/show/996-14 (дата звернення: 25.11.2024).

9. Штангрет А. М., Караїм М. М. Обліково-аналітичне забезпечення як основа прийняття рішень суб'єктами безпеки підприємств. Електрононний науково-практичний журнал «Східна Європа: Економіка, бізнес та управління».

2020 № 2(07). С. 167–170. URL : http://www.easterneurope-ebm.in.ua/index.php/vipusk-2-2017 (дата звернення: 25.11.2024).

10. Штангрет А. М. Процес здійснення обліково-аналітичного забезпечення управління економічною безпекою підприємства. Наукові записки Української академії друкарства. Серія : Економічні науки. 2019. №2. С. 15–22.

11. Lipych L., Skoruk O. Providing financial and economic security of the enterprise in the conditions of development of the digital economy. Економічнийчасопис Східноєвропейського національного університету імені Лесі Українки : журнал / уклад. Любов Григорівна Ліпич, Мирослава Богданівна Кулинич. Луцьк : Вежа-Друк, 2020. № 3. С. 106–113.

12. Skoruk O. Cechy systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie. Соціально-компетентне управління корпораціями в умовах поведінкової економіки : матеріали Міжн. наук.-практ. конф. присв. 25 річниці створення СНУ імені Лесі Українки (Луцьк, 28 листопада 2018 р.) / відп. ред. О. М. Полінкевич, Л. В. Шостак. Луцьк, 2019. С. 437–439.

13. Economic Security: Neglected Dimension of Security / Center for Strategic Conferencing, Institute for National Strategic Studies. – Defense University, Washington, D. C. 2021. 130 p.

14. Leveson I. Economic Security: A Guide for an Age of Insecurity / Universe. 2021. 654 p.

15. Скорук О. В. Обліково-аналітичне забезпечення економічної безпеки підприємства: конспект лекцій. Луцьк : Волинський національний університет імені Лесі Українки, 2021. 94 с.

16. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.

17. Цифрова безпека на персональному рівні. URL: https://learn.ztu.edu.ua/pluginfile.php/367828/mod_resource/content/0/%D0%A2%D0

%B5%D0%BC%D0%B0%203_%D0%B7%D0%B0%D0%BA%D1%96%D0%BD%D1%87%D0%B5%D0%BD%D0%BD%D1%8F.pdf (дата звернення: 25.11.2024).

18. Цифрова та інформаційна безпека : Рекомендований перелік онлайн-курсів / КЗ «ЗОУНБ» ЗОР, Регіон. консультаційно-тренінг. центр ; [уклад. Г. Мацієвська]. - Запоріжжя : [ЗОУНБ], 2023. 15 с.

19. Белл Д. Настання постіндустріального суспільства. Філософія: хрестоматія (від витоків до сьогодення): навч. посіб. / за ред. акад. НАН України Л. В. Губерського. Київ : Знання, 2019. С. 419–431.

20. Давидова Л. Цифрова безпека та нові медіа. URL : https://www.facebook.com/luddavidova/posts/4700603449995998.

21. Зайко Л. Цифрова безпека як складник професійної діяльності журналістів нових медіа. URL : https://www.facebook.com/permalink.php?story_fbid=2979765235622107&id=100007659795822 (дата звернення: 25.11.2024).

22. Мей К. Інформаційне суспільство. Скептичний погляд : пер. з англійської. Київ : «К.І.С.», 2004. XIV с., 220 с.

23. Мороз В. Яким українським компаніям можна довіряти свої персональні дані. НВ Бізнес. 2021. 4 жовт. URL : https://biz.nv.ua/ukr/experts/zahist-personalnih-danih-v-ukrajinskih-kompaniyahrezultati-doslidzhennya-novini-ukrajini-50187153.html (дата звернення: 25.11.2024).

24. Лутковська В. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання праві свобод людини і громадянина в Україні. Права людини. Київ, 2019. 627 с.

25. Recommendation CM/Rec (2018) 2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies). URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14 (дата звернення: 25.11.2024).

26. Стратегія гендерної рівності Ради Європи на 2018−2023 рр. 51 с. URL: https://rm.coe.int/strategy-en2018-2023/16807b58eb

25. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р. URL: http://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 25.11.2024).

26.Золотар О. Інформаційна безпека людини: теорія і практика: монографія. Київ: «Тов. Видавничий дім «АртЕк», 2018. 446 с.

27. Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язкуз опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: http://zakon.rada.gov.ua/laws/show/984_008-16 (дата звернення: 25.11.2024).

28. On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA: Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2020 . URL: https:///eur-lex.europa.eu/legalcontent/en/TXT/%3Furi%3DCELEX%253A32016L0680&prev=search (дата звернення: 25.11.2024).

29. On the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime: Directive (EU) 2016/681 of the European Parliament and of the Council, of 27 April 2016. URL: https://consilium.europa.eu/en/press/press-releases/2016/04/21-council-adopts-eu-pnr-directive/&prev=search (дата звернення: 25.11.2024).

30. Про захист персональних даних: Закон України від 1.07.2010 р. URL: http://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 25.11.2024).

31. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковий протокол до

32. Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних від 28.01.1981 р. URL: http://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 25.11.2024).

32. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 25.11.2024).

33. Рекомендація NR(99) 5 Комітету Міністрів державам-членам Ради Європи «Про захист недоторканності приватного життя в Інтернеті» від 23.02.1999 р. URL: http://zakon.rada.gov.ua/laws/show/994_357 (дата звернення: 25.11.2024).

34. ТСН. Політика конфіденційності та захисту персональних даних. URL: https://tsn.ua/privacy-policy (дата звернення: 25.11.2024).

35. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник / М.В. Бем, І.М. Городиський, Г. Саттон, О.М. Родіоненко. К.: К.І.С., 2015. 220 с.

36. Active Directory overview. URL: https://learn.microsoft.com/uk-ua/troubleshoot/windows-server/active-directory/active-directory-overview (дата звернення: 25.11.2024).

37. VeraCrypt / BitLocker / PGP (Pretty Good Privacy). URL: https://en.wikipedia.org/wiki/Pretty_Good_Privacy (дата звернення: 25.11.2024).

38. Veeam Backup & Replication / Acronis Backup / Commvault. URL: https://www.peerspot.com/products/comparisons/acronis-cyber-protect_vs_commvault-complete-data-protection_vs_veeam-backup-replication (дата звернення: 25.11.2024).

39. Splunk / SolarWinds / Nagios. URL: https://www.quora.com/What-is-the-difference-between-Splunk-and-Nagios (дата звернення: 25.11.2024).

40. Kaspersky Endpoint Security / Bitdefender / Symantec Endpoint Protection. URL: https://www.bitdefender.com/business/support/en/77212-376350-software-incompatible-with-best.html (дата звернення: 25.11.2024).

41. Булдижов В. Кібербезпека, ІБ, безпека ІТ – у чому різниця? URL:

https://www.h-x.technology/ua/blog-ua/infosec-itsec-cybersecurity-defference-ua (дата звернення 20.10.2024).

42. ISO/IEC 27001:2022. Інформаційна безпека, кібербезпека та захист конфіденційності – Системи управління інформаційною безпекою – Вимоги. URL: https://www.iso.org/standard/27001

43. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: постанова КМ від 19 червня 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення 17.11.2024 р.).

44. Про прийняття національних стандартів, зміни до національного стандарту та скасування національних стандартів: наказ ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» № 210 від 17.08.2023 р. URL: https://zakon.rada.gov.ua/rada/show/v0210774-23#Text (дата звернення 17.11.2024 р.).

45. Про перелік відомостей, що не становлять комерційної таємниці: постанова Кабінету Міністрів України № 611 від 09.08.1993 р. URL: http://zakon2.rada.gov.ua/laws/show/611-93-%D0%BF (дата звернення 17.11.2024 р.).

46. Про захист від недобросовісної конкуренції: закон України № 236/96-ВР від 07.06.1996 р. URL: https://zakon.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80#Text (дата звернення 17.11.2024 р.).

47. Про інформацію: закон України № 1703-IV від 11.05.2004 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 17.11.2024 р.).

48. Фатенок-Ткачук, А., Скорук О., Януш, Р., & Захарчук І. (2024). Використання штучного інтелекту в обліково-аналітичних процесах. *Економічний часопис ВНУ ім. Лесі Українки*. 2024. № 2. С.21–29. https://doi.org/10.29038/2786-4618-2024-02-21-29.

49. Кулинич М. Б., Фатенок-Ткачук А. О., Мельник К. П. Облік, аналіз, аудит і оподаткування в управлінні розвитком суб'єктів господарювання через призму цифровізації : монографія. Луцьк : Вежа-Друк, 2021. 170 с. / Алла

Фатенок-Ткачук. Обліково-аналітичне забезпечення стратегічного планування у системі стратегічного управління розвитком підприємства. С.39–123.

50. Gridlex Sky Accounting, Expenses & ERP Software. Gridlex - CRM, Help Desk, HRMS, Expenses, Accounting &ERP. URL: https://gridlex.com/c/sa/?utm_source=gAAAAABky44FxvzHaG41QvQ5l4bR9bONczUZ7WIjQ4aqe7NuSgB0xgx3I6_qW9gGtR_ExeohyIKvpoGIoMMSqzq3qoGqgZm5wA== (дата звернення: 08.03.2024).

51. Financial Operations: Bookkeeping For Modern Startups. Financial Operations: Bookkeeping For Modern Startups. URL: https://www.zeni.ai/ (дата звернення: 08.03.2024).

52. BILL Spend & Expense (Formerly Divvy). BILL | Financial Operations Platform for Businesses & Firms. URL: https://www.bill.com/product/spend-and-expense (дата звернення: 08.03.2024).

53. Botkeeper | Bookkeeping for Accounting Firms. *Botkeeper | Bookkeeping for Accounting Firms*. URL: https://www.botkeeper.com/ (дата звернення: 27.02.2024).

54. Ahmed Hamdi, Elodie Carel, Aurélie Joseph, Mickael Coustaty, Antoine Doucet. Information Extraction from Invoices. International Conference on Document Analysis and Recognition ICDAR 2021, Sep 2021, Lausanne, Switzerland. pp.699-714, ⟨10.1007/978-3-030-86331-9_45⟩. ⟨hal-03418385⟩(дата звернення: 27.02.2024).

55. Колесник П. А. Кіберзахист обєктів критичної інфраструктури у контексті безпеки цифрових даних. *Сучасні тенденції розвитку обліку, аналізу, контролю, аудиту та оподаткування*: матеріали V науково-практичної міжнародної конференції (21 листопада 2024 р., м. Луцьк). – Луцьк : ВНУ імені Лесі Українки, 2024. URL: http://surl.li/tenfff