НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки / інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ НА ПІДПРИЄМСТВІ, НА ПРИКЛАДІ HERAEUS GROUP»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 07 «Управління та адміністрування»,
спеціальність 73 «Менеджмент»
Пейдж Нікіта Ендрю

Керівник: професор, д.е.н.
Горбаченко Станислав Анатолійович

Рецензент: доктор філософії,
Слатвінська Валерія Миколаївна

Одеса - 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **07 Управління та адміністрування**
Спеціальність: **073 Менеджмент**
Назва освітньої програми: **ІТ менеджмент та маркетинг**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Пейдж Нікіті Ендрю

1. Тема роботи: «Впровадження системи управління кібербезпекою на підприємстві, на прикладі компанії Heraeus group»
Керівник роботи: професор, д.е.н. Горбаченко Станислав Анатолійович
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «21» травня 2025 рік
3. Дата видачі завдання «16» вересня 2024 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1.	Аналіз теми та формування завдання	20.09. 2024 -30.09.2024	
2.	Огляд літератури та нормативно-правової бази	1.10.2024 -11.10.2024	
3.	Аналіз діяльності Heraeus Group	12.10.2024 -15.11.2024	
4.	Розробка рекомендацій щодо системи управління кібербезпекою	16.11.2024 - 27.01.2025	
5.	Оцінка ефективності впровадження	29.01. 2025 - 04.03.2025	
6.	Оформлення та редагування роботи	05.03.2025 - 22.04.2025	
7.	Підготовка до захисту	02.05.2025 - 19.05.2025	
8.	Захист	13.05.25	

Здобувач_____
(підпис) (прізвище та ініціали)
Керівник роботи_____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Впровадження системи управління кібербезпекою на підприємстві, на прикладі компанії Heraeus Group» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 073 Менеджмент, галуззю знань 07 «Управління та адміністрування», містить 2 рисунки, 24 таблиці, 71 джерело за переліком посилань. Робота виконана на 63 сторінках, з яких 49 – основного тексту.

Метою роботи є розробка практичних рекомендацій щодо вдосконалення системи управління кібербезпекою на основі аналізу діяльності компанії Heraeus Group. У роботі досліджено теоретичні засади кібербезпеки, міжнародні стандарти (ISO/IEC 27001, NIST, GDPR), проаналізовано IT-інфраструктуру компанії (понад 2000 серверів, 14000 користувачів) та статистику кіберінцидентів за 2021–2023 роки. На основі SWOT-аналізу виявлено ключові вразливості та розроблено стратегію підвищення кіберзахисту, що включає модернізацію SCADA-систем, впровадження архітектури zero-trust, аутсорсинг, оптимізацію процесів та навчання персоналу. Проведено економічну оцінку ефективності запропонованих заходів через показник ROI.

Результати дослідження можуть бути використані промисловими підприємствами для посилення кіберзахисту, оптимізації витрат та забезпечення відповідності міжнародним стандартам. Рекомендації мають цінність для формування культури безпеки та адаптації до умов цифрової трансформації, зокрема в Україні.

Можливими напрямами подальших досліджень є використання квантової криптографії, блокчейну та хмарних рішень для підвищення надійності інформаційної інфраструктури.

КІБЕРБЕЗПЕКА, HERAEUS GROUP, ІНФОРМАЦІЙНА БЕЗПЕКА, РИЗИКИ, ROI, ЦИФРОВА ТРАНСФОРМАЦІЯ

ANNOTATION

The thesis on the topic “Implementation of a Cybersecurity Management System at an Enterprise, Using the Example of Heraeus Group” is submitted for obtaining the first (bachelor’s) level of higher education in the specialty 073 Management, field of knowledge 07 “Management and Administration”. It contains 2 figures, 24 tables, and 71 references. The work spans 63 pages, of which 49 are the main text.

The purpose of the study is to develop practical recommendations for improving the cybersecurity management system based on an analysis of Heraeus Group’s operations. The work examines the theoretical foundations of cybersecurity, international standards (ISO/IEC 27001, NIST, GDPR), and analyzes the company’s IT infrastructure (over 2,000 servers, 14,000 users) and cyber incident statistics for 2021–2023. Based on a SWOT analysis, key vulnerabilities were identified, and a strategy to enhance cybersecurity was developed, including SCADA system modernization, implementation of zero-trust architecture, outsourcing, process optimization, and staff training. The economic effectiveness of the proposed measures was evaluated using the ROI metric.

The research results can be applied by industrial enterprises to strengthen cybersecurity, optimize costs, and ensure compliance with international standards. The recommendations are valuable for fostering a security culture and adapting to digital transformation conditions, particularly in Ukraine.

Potential directions for further research include the use of quantum cryptography, blockchain, and cloud solutions to enhance the reliability of information infrastructure.

CYBERSECURITY, HERAEUS GROUP, INFORMATION SECURITY, RISKS, ROI, DIGITAL TRANSFORMATION

ЗМІСТ

ВСТУП

Актуальність теми зумовлена стрімкою діджиталізацією бізнесу та зростанням кіберзагроз, які вже входять до топ-5 глобальних ризиків (WEF, 2024). Очікується, що світові збитки від кіберзлочинності сягнуть $10,5 трлн на рік до 2025 року (Cybersecurity Ventures).

Особливо гостро проблема стоїть в умовах воєнного стану в Україні - кількість кібератак зросла у 4 рази. Збільшення атак на промисловий сектор (на 300% за 2019-2023, за IBM) також пов’язане з впровадженням IoT, хмарних сервісів і ШІ.

Успішна атака може спричинити мільйонні збитки. Відповідність стандартам ISO/IEC 27001 та GDPR дозволяє зменшити ризики, підвищити рівень захисту й репутацію компанії. Це підкреслює потребу в системному дослідженні механізмів кібербезпеки та стратегій захисту інформаційних активів.

Метою цього дослідження є розроблення практичних рекомендацій з адаптації міжнародного досвіду кібербезпеки компанії Heraeus Group до умов вітчизняного підприємницького середовища.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- проаналізувати поняття кібербезпеки та ключові елементи системи її менеджменту в умовах цифрової трансформації бізнесу;
- дослідити теоретичні основи забезпечення інформаційної безпеки підприємств;
- оцінити вплив рівня кіберзахисту на ефективність діяльності компанії Heraeus Group;
- здійснити економічний аналіз витрат на кібербезпеку та ефективності інвестицій у захисні заходи;
- розробити стратегію підвищення кібербезпеки Heraeus Group з урахуванням сучасних загроз і вимог до безпеки інформаційної інфраструктури.

Методологічною основою дослідження є наукові праці вітчизняних та зарубіжних учених у сфері кібербезпеки, зокрема праці Бурячка В. Л., Гнатюка С. О., Корченка Д. В., Гулака Г. М., Корченка О. Г., Терейковського І., Онищенка Ю.М., а також зарубіжних дослідників С. МакКлюр, К. Соналі, Р. Девіс, А. Хушнуд, Л. Більге, П. Кім, С. Самікша, К. Стоуффер, С. Клеменс, Ф. Мізрак, А. Глохем, А. Мескіда та інші. Дослідження ґрунтується на системному підході з використанням комплексу методів: системного аналізу - для вивчення структури кібербезпеки, порівняльного - для аналізу міжнародного досвіду, статистичного - для оцінки ефективності заходів, експертного - для аналізу ризиків, та економіко-математичного моделювання - для розробки практичних рекомендацій.

Методологія дослідження базується на комплексному підході: теоретичні методи використано для аналізу літератури й нормативних документів, емпіричні — для збору даних про кіберзагрози, економічні — для оцінки ефективності заходів, а стратегічні — для формування рекомендацій щодо розвитку кібербезпеки Heraeus Group.

Наукова новизна полягає в удосконаленні підходів до управління кібербезпекою з урахуванням міжнародного досвіду та специфіки глобального й українського бізнес-середовища:

-проведено системний аналіз кібербезпеки в умовах цифрової трансформації та визначено ключові елементи її менеджменту для промислових підприємств;

-теоретично обґрунтовано засади інформаційної безпеки з урахуванням сучасних викликів;

-вперше досліджено зв’язок між рівнем кіберзахисту, безперервністю бізнес-процесів і ефективністю діяльності (на прикладі Heraeus Group);

-оцінено ефективність заходів протидії кіберризикам з урахуванням витрат, збитків та окупності інвестицій;

-запропоновано адаптивну модель стратегії кіберзахисту, придатну для українських компаній.

Рекомендації враховують виклики цифровізації, глобалізації та вплив людського фактору.

Практичне значення роботи полягає в можливості застосування її результатів для підвищення кібербезпеки українських підприємств. Рекомендації щодо впровадження системи управління кібербезпекою можуть бути адаптовані до різних галузей. Досвід Heraeus Group слугує прикладом для оптимізації витрат, зменшення кіберризиків і вдосконалення захисту інформаційних активів. Запропоновані інструменти, адаптовані до українських умов, сприятимуть підвищенню ефективності систем кіберзахисту.

Апробація результатів почала здійснюватися з другого курсу через виступи на всеукраїнських і міжнародних конференціях, з подальшими публікаціями в наукових збірниках та журналах категорії Б.

1. Пейдж Нікіта Ендрю. Державно-правова база легітимізації боротьби з кіберзлочинами. Національний університет «Одеська юридична академія»: Матеріали Всеукраїської науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» 25 листопада 2022 року, м. Одеса, 2022. С. 191-193.

2. Nikita Andrew Page. Music information as a factor of progress in educational institutions of England. Міжнародна науково-творча конференція «Захід-Схід: культура та мистецтво. Пам’яті видатних митців України присвячується, 25-26 вересня 2022 року, м. Одеса. Збірник наукових праць. С.182-185.

3. Page Nikita Andrew. Technologies through the prism of human values and organizational culture. Міжнародний Фестиваль-Конференція «Захід - Схід: культура і сучасність - на славу знаних митців Одеси», 28-29 вересня 2024 року, м. Одеса. Збірник наукових праць. С.201-204.

4. Page N. A. Corporate Philosophy and Culture: The Role and Functions of a Manager. Міжнародна науково-творча конференція трансформація музичної культури і освіти: пам’яті витоків і звершень першого музичного ВИШУ України, 11-13 травня 2024 року, м. Одеса. 2024. С. 280-283.

5. Page Nikita Andrew. The impact of hybrid threats on the cyber security of critical infrastructure in the context of modern global challenges. Національний університет «Одеська юридична академія»: Матеріали Всеукраїської науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики», 22 листопада 2024 року, м. Одеса, 2024. С. 161-163.

6. Горбаченко С. А., Пейдж Н. Е. Цифрова трансформація управління персоналом у Industry 5.0: біоцентричний підхід. Харків, Державний біотехнологічний університет: Журнал з менеджменту, економіки та технологій, 2025. Вип. 1. С. 275-285. DOI: https://doi.org/10.69803/3083-6034-2025-1-275

Структура роботи обумовлена метою та завданнями дослідження. Структура дослідження - робота складається з вступу, трьох розділів, висновків до кожного розділу, загальних висновків, списку використаних джерел та додатків. Основний текст складає 59 сторінок, список використаної літератури включає 71 найменування. Дипломна робота включає в себе 24 таблиці та 2 рисунка.

Інформаційною базою дослідження є наукові публікації та монографічні видання вітчизняних і закордонних учених, нормативно-законодавчі акти України, Великобританії, США та інших країн, нормативні акти компанії, матеріали наукових досліджень, викладок, що проводились безпосередньо у компанії Heraeus Group

1 ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

1.1 Роль кібербезпеки в сучасному глобальному бізнес-середовищі на прикладі компанії Heraeus Group

У сучасну епоху цифрової трансформації кібербезпека перетворилася на стратегічний пріоритет для міжнародних компаній, особливо в технологічно складних і динамічних галузях. Це не просто набір технічних заходів, а комплексна, багатовимірна система управління ризиками, що впроваджується на всіх рівнях корпоративної структури [50, 6]. Досвід показує, як кібербезпека впливає на стабільність, конкурентоспроможність і стійкість бізнесу в умовах глобалізації, цифровізації та постійного зростання кіберзагроз.

Міжнародні компанії з тривалою історією, що спеціалізуються на високотехнологічних галузях, неминуче стикаються з високими кіберризиками, пов'язаними з розгалуженою мережею постачальників, великою кількістю співробітників та складною IT-інфраструктурою.

У світлі таких викликів впроваджуються комплексні багаторівневі системи кіберзахисту, які охоплюють технологічні, організаційні та людські аспекти. Особлива увага приділяється не лише захисту виробничих процесів та IT-інфраструктури, а й збереженню інтелектуальної власності, безпеці персональних даних клієнтів і співробітників, а також безперервності бізнесу в умовах потенційних кібератак [50, 6; 65].

Цифровізація виробництва, активне впровадження концепції Індустрії 4.0, використання штучного інтелекту й машинного навчання у виробничих процесах - усе це створює новий рівень складності в управлінні кібербезпекою. Інтеграція промислових систем із цифровими платформами призводить до появи нових вразливостей, зокрема у SCADA-системах та промислових контролерах, де навіть незначне втручання може спричинити порушення технологічного процесу з катастрофічними наслідками [61, 22-33].

У цьому контексті важливим є те, що кібербезпека не розглядається як вузько спеціалізована IT-проблема, а розглядається з позицій стратегічного управління. Впроваджуються передові системи виявлення загроз,

автоматизовані засоби моніторингу, проводиться постійне навчання персоналу, а також підтримуються партнерства з міжнародними організаціями в галузі кібербезпеки [33, 8-9; 67].

Особливо показовим є підхід до загроз, що постійно еволюціонують. Наприклад, цільові атаки (APT), які зазвичай реалізуються організованими групами з підтримкою держав або конкурентів, становлять серйозну небезпеку для високотехнологічних компаній через їх технологічну спеціалізацію та масштабні інвестиції в наукові дослідження. Подібні атаки є прихованими, довготривалими та здебільшого націленими на викрадення інновацій та технічної документації, зокрема в наукомістких галузях [49, 1-12].

Програми-вимагачі нового покоління також набули широкого розповсюдження. Сучасні підприємства фіксують спроби подібних атак, які передбачають не лише шифрування корпоративних даних, але й загрозу їх оприлюднення. Слід наголосити, що найбільшу вразливість виявляють системи управління виробництвом та автоматизовані лінії, що можуть бути виведені з ладу навіть короткочасною атакою.

Не менш небезпечним є промисловий кібершпигунство, зокрема через фішингові кампанії та атаки соціальної інженерії, які часто націлюються на дослідницькі підрозділи та топ-менеджмент компаній. Ці загрози особливо критичні, враховуючи унікальність розробок, що здійснюються в рамках науково-дослідної діяльності [43, 5-26].

Також варто зазначити, що підприємства стикаються з атаками на хмарну інфраструктуру, системи резервного копіювання, системи управління доступом та навіть мобільні пристрої співробітників. Зокрема, із впровадженням моделей віддаленої роботи під час пандемії COVID-19, було переглянуто політики безпеки та посилено захист каналів дистанційного доступу.

Не менш серйозною проблемою залишаються DDoS-атаки, що можуть блокувати корпоративні веб-ресурси, порушуючи як внутрішню комунікацію, так і зовнішні бізнес-процеси. Системи електронного документообігу та цифрові підписи також перебувають у зоні ризику, особливо враховуючи сучасні методи підробки документів.

Додатково, загрози для IoT-пристроїв, які активно використовуються у виробництві, а також для систем штучного інтелекту та машинного навчання, зростають пропорційно до рівня цифрової трансформації. Атаки можуть бути спрямовані на маніпуляції алгоритмами прийняття рішень, що, у свою чергу, загрожує порушенням контролю якості продукції та безпеки технологічних процесів.

Систематизація виявлених типів загроз показує, що підприємства стикаються з широким спектром кіберризиків, які потребують постійного вдосконалення стратегії захисту. З цією метою інвестуються кошти в оновлення інфраструктури, впроваджуються криптографічні рішення нового покоління, відбувається адаптація до викликів, пов'язаних із квантовими обчисленнями, та впроваджуються протоколи відповідності таким нормативним актам, як GDPR, CCPA тощо [31, 1-10; 32, 43-45; 59, 80813-80828].

Підсумовуючи, можна стверджувати, що в сучасному глобалізованому бізнес-середовищі кібербезпека є не просто інструментом забезпечення стабільної роботи, а й запорукою довготривалого успіху, збереження конкурентних переваг і захисту інтересів як компанії, так і її клієнтів. Практика підтверджує, що лише комплексний підхід, який охоплює всі рівні корпоративної структури, від технічного до стратегічного, дозволяє ефективно протистояти кіберзагрозам та зберігати стійкість у світі цифрових викликів.

1.2 Ключові елементи системи менеджменту кібербезпеки

У сучасних умовах цифровізації та глобалізації система менеджменту кібербезпеки в міжнародних технологічних компаніях стала невід'ємною частиною корпоративного управління. Вона виконує роль стратегічного механізму, який не лише захищає інформаційні активи, але й інтегрується у всі бізнес-процеси, забезпечуючи стійкість компанії до кіберзагроз.

Стратегічне планування є фундаментальним елементом цієї системи, оскільки дозволяє узгоджувати заходи кіберзахисту з загальними цілями компанії. Таке інтегроване планування дає змогу оптимально розподіляти ресурси,

прогнозувати потенційні ризики та оперативно реагувати на зміни в інформаційному середовищі. Важливим аспектом є те, що кібербезпека перестає бути виключно технічним питанням - вона стає частиною корпоративної культури та бізнес-стратегії.

Організаційна структура управління кібербезпекою в таких компаніях будується на чіткому розподілі ролей та відповідальностей. Ключову позицію займає головний директор з інформаційної безпеки (CISO), який безпосередньо підпорядкований топ-менеджменту компанії [37, 251-276]. Така модель управління забезпечує оперативне прийняття рішень та ефективну комунікацію між технічними фахівцями та керівництвом. Паралельно проводиться регулярна оцінка ризиків, яка включає не лише технічний аудит, але й аналіз потенційних загроз для критичної інфраструктури та інтелектуальної власності компанії [21, 17-19; 66].

Технічна складова системи постійно еволюціонує, що обумовлено динамічним розвитком кіберзагроз. Сучасні технології захисту мереж, системи виявлення вторгнень та механізми контролю доступу, побудовані на принципі найменших привілеїв, утворюють багаторівневий захист. Особливу увагу приділяється автоматизації процесів моніторингу та аналізу безпекових подій, що дозволяє виявляти аномалії в режимі реального часу.

Реагування на інциденти є критично важливим компонентом системи. Міжнародні компанії створюють спеціалізовані команди реагування (CERT), які працюють цілодобово та діють за чіткими протоколами [46, 235-248]. Такі команди не лише ліквідують наслідки атак, але й проводять постінцидентний аналіз, що дозволяє вдосконалювати захист.

Важливим напрямом є розвиток кадрового потенціалу. Регулярні тренінги з кібербезпеки для співробітників усіх рівнів допомагають формувати культуру безпеки та знижувати ризики, пов'язані з людським фактором. При цьому навчальні програми постійно оновлюються, враховуючи актуальні загрози та специфіку різних відділів компанії.

Умови глобальної економіки вимагають особливої уваги до кіберризиків у ланцюгах постачання. Компанії встановлюють жорсткі вимоги до партнерів

щодо захисту інформації та реалізують механізми безпечного обміну даними. Це дозволяє мінімізувати ризики, пов'язані з третіми сторонами.

Вся діяльність у сфері кібербезпеки базується на міжнародних стандартах, зокрема ISO 27001, що забезпечує системність підходу та постійне вдосконалення [39, 3-17]. Для підтримки безперервності бізнесу розробляються комплексні плани аварійного відновлення, які регулярно тестуються. Оцінка ефективності заходів здійснюється через систему ключових показників (KPI), що дозволяє вимірювати рівень захисту та визначати пріоритетні напрями розвитку [55, 12-20; 70].

Міжнародні компанії успішно поєднують глобальні стандарти з локальними вимогами, адаптуючи свої системи кібербезпеки до законодавства конкретних країн. Такий гнучкий підхід дозволяє ефективно працювати на різних ринках, зберігаючи високий рівень захисту.

Таким чином, сучасна система менеджменту кібербезпеки в міжнародних технологічних компаніях є комплексною та динамічною. Вона поєднує стратегічне планування, технічні рішення, організаційні механізми та роботу з персоналом, створюючи надійний захист у постійно змінюваному цифровому середовищі.

1.3 Стратегія нормативно-правового регулювання кібербезпеки в Україні та світі

У контексті питань нормативно–правового регулювання кібербезпеки на національному та міжнародному рівнях необхідно відзначити наявність багаторівневої системи законодавчих актів, яка охоплює як загальнодержавні положення, так і специфічні норми, що стосуються окремих секторів економіки, типів даних або технологій. Такий підхід є критично важливим для ефективного управління кіберризиками та забезпечення стійкості організацій до сучасних кіберзагроз.

В Україні основними документами, що визначають нормативну основу у сфері кібербезпеки, є Закон України «Про основні засади забезпечення

кібербезпеки України» та Стратегія кібербезпеки України. Ці документи формують фундаментальну правову та організаційну основу для побудови системи кіберзахисту як у державному, так і в приватному секторі. Вони визначають функції основних суб'єктів національної системи кібербезпеки, порядок взаємодії між ними, а також орієнтири для формування внутрішніх політик інформаційної безпеки в організаціях [10, 1–17].

На міжнародному рівні важливу роль відіграє Загальний регламент про захист даних (GDPR) Європейського Союзу, який встановлює жорсткі вимоги до збирання, обробки та зберігання персональних даних. GDPR зобов'язує організації впроваджувати комплексні системи управління персональними даними, призначати відповідальних осіб - DPO (Data Protection Officer) - і забезпечувати прозорість обробки даних [35, 1–23].

У США регулювання здійснюється на кількох рівнях - федеральному та рівні окремих штатів. Такі нормативні акти, як California Consumer Privacy Act (CCPA) та SHIELD Act штату Нью–Йорк, визначають обов'язки компаній у сфері захисту персональної інформації та передбачають жорсткі санкції за порушення [39, 7–19].

Одним із ключових елементів відповідності міжнародним вимогам є сертифікація ISO/IEC 27001 - стандарту, що регламентує створення систем управління інформаційною безпекою (СУІБ) в організаціях. Цей стандарт має універсальне значення для компаній у різних галузях, оскільки дозволяє системно підходити до управління ризиками в інформаційній сфері [39, 7–19].

У специфічних сферах, таких як виробництво медичних виробів, важливим є дотримання вимог Регламенту ЄС щодо медичних засобів, а також наглядових норм FDA (США). Ці документи висувають підвищені вимоги до кібербезпеки медичних пристроїв як елементів критичної інфраструктури.

В Азійсько-Тихоокеанському регіоні спостерігається тенденція до локалізації міжнародних стандартів кібербезпеки відповідно до національного законодавства – це зумовлено як політичною специфікою країн, так і рівнем цифровізації суспільства [58, 387–411; 69]. Водночас зростає роль стандарту

ISA/IEC 62443 – міжнародного документа, що регламентує вимоги до безпеки промислових систем управління та автоматизації [38, 196–210].

Додаткову гарантію безперервності функціонування організацій забезпечує стандарт ISO 22301, який встановлює принципи управління безперервністю бізнесу – зокрема, у випадку кіберінцидентів, техногенних катастроф або воєнних дій [24, 83–90].

Варто також враховувати роль Закону Сарбейнса-Окслі (Sarbanes-Oxley Act), що має значення для публічних компаній та регламентує забезпечення достовірності фінансової звітності, у тому числі шляхом впровадження інформаційних контролів [57, 10–15].

В умовах воєнного стану в Україні спостерігається активізація нормативного регулювання - посилюються вимоги до обміну інформацією з правоохоронними органами, впроваджуються додаткові заходи безпеки щодо захисту критичної інфраструктури та промислових об’єктів [34, 50–71].

Таким чином, ефективне нормативно–правове регулювання кібербезпеки базується на багаторівневому, адаптивному підході, що передбачає синхронізацію національних положень із міжнародними стандартами, врахування специфіки окремих галузей, а також адаптацію до геополітичних реалій та динамічного розвитку цифрових технологій.

2 КІБЕРБЕЗПЕКА ПІДПРИЄМСТВА У КОНТЕКСТІ ГЛОБАЛЬНИХ ЗАГРОЗ НА ПРИКЛАДІ КОМПАНІЇ HERAEUS GROUP

2.1 Загальна характеристика компанії Heraeus Group та її IT-інфраструктури

Міжнародна компанія Heraeus Group - це глобальна німецька технологічна група, заснована в 1851 році, яка пройшла шлях трансформації від локальної аптеки в Ханау до світового лідера у сфері високих технологій. На сьогодні компанія має представництва у понад 40 країнах світу та спеціалізується на виробництві й обробці дорогоцінних металів, медичних технологіях, виробництві кварцового скла та інших високотехнологічних напрямках діяльності.

Організаційна структура Heraeus Group побудована за матричним принципом і включає різноманітні бізнес-підрозділи, серед яких Heraeus Electronics, Heraeus Medical Components, Heraeus Precious Metals та інші. Варто зауважити, що компанія постійно інвестує в дослідження та інновації, щорічно отримуючи сотні нових патентів.

IT-інфраструктура компанії є комплексною системою, що забезпечує ефективну роботу всіх підрозділів. Вона включає розгалужену мережеву інфраструктуру, потужну серверну базу та сучасні системи зберігання даних. Зокрема, прикладні системи компанії складаються з ERP-системи SAP, систем управління виробництвом, документообігом та інших бізнес-процесів [40, 144; 68].

Крім того, Heraeus Group активно впроваджує інноваційні технології, такі як штучний інтелект, машинне навчання та Інтернет речей для оптимізації виробничих процесів та предиктивної аналітики. При цьому, компанія використовує гібридну хмарну інфраструктуру та мікросервісну архітектуру, що забезпечує високий рівень відмовостійкості, масштабованості та безпеки системи [47, 239-245]. Таблиця 2.1 демонструє вражаючі показники великої міжнародної компанії з річним оборотом у 29,1 мільярдів євро. Ця організація має значний масштаб діяльності, що підтверджується не лише фінансовими

показниками, але й штатом у понад 16 200 співробітників та широкою географічною присутністю - більше 100 локацій у понад 40 країнах світу.

Таблиця 2.1 – Основні показники діяльності компанії Heraeus Group за 2023 рік

Показник	Значення
Річний оборот	29,1 млрд. євро
Кількість співробітників	16200 осіб
Кількість локацій	>100
Країни присутності	<40
Кількість IT-користувачів	>14000
Серверна інфраструктура	>2000 серверів

Джерело: розраховано автором самостійно на основі архівних документів компанії Heraeus Group

Таблиця 2.1 демонструє вражаючі показники великої міжнародної компанії з річним оборотом у 29,1 мільярдів євро. Ця організація має значний масштаб діяльності, що підтверджується не лише фінансовими показниками, але й штатом у понад 16 200 співробітників та широкою географічною присутністю - більше 100 локацій у понад 40 країнах світу.

Особливо привертає увагу високий рівень діджиталізації компанії, про що свідчить кількість IT-користувачів (більше 14 000) та розвинена інфраструктура, що включає понад 2 000 серверів. Варто зауважити, що співвідношення IT-користувачів до загальної кількості працівників (14 000 з 16 200) вказує на майже повну залученість персоналу до роботи з інформаційними системами, що безумовно відображає високий ступінь автоматизації бізнес-процесів у компанії. Показники в таблиці 2.2 демонструє розподіл IT-бюджету компанії, який складає 150 мільйонів євро. Найбільша частка коштів (30% або 45 мільйонів євро) спрямовується на програмне забезпечення, що свідчить про високу залежність бізнес-процесів від якісного софту. Друге місце посідають витрати на апаратне забезпечення - 25% бюджету (37,5 мільйонів євро), що вказує на постійну модернізацію технічної інфраструктури.

Таблиця 2.2 – Розподіл IT-бюджету компанії Heraeus Group, 2023 рік

Категорія витрат	Частка бюджету (%)	Сума (млн євро)
Апаратне забезпечення	25%	37,5
Програмне забезпечення	30%	45,0
IT-послуги	20%	30,0
Персонал	15%	22.5
Кібербезпека	10%	15,0
Всього	100%	150,0

Джерело: розраховано автором самостійно на основі архівних документів Heraeus Group

IT-послуги займають третю позицію з часткою 20% (30 мільйонів євро), а на персонал виділяється 15% бюджету (22,5 мільйонів євро). Варто зауважити, що компанія окремо виділяє 10% бюджету (15 мільйонів євро) на кібербезпеку, що підкреслює серйозне ставлення організації до захисту інформаційних систем.

Такий розподіл бюджету є характерним для сучасної компанії, яка розуміє значення цифрової трансформації. Узагальнюючи результати аналізу, можна відзначити, що витрати на одного IT-користувача становлять 10 714 євро на рік, а коефіцієнт серверного навантаження дорівнює 7 користувачів на сервер. Ці показники додатково підтверджують високий рівень технологічного розвитку компанії.

Показники в таблиці 2.3 дають нам уявлення про масштаб технічної інфраструктури компанії. Отже, організація має чотири стратегічно розташованих центри обробки даних у ключових регіонах світу - Німеччині, США, Китаї та Сінгапурі, що забезпечує глобальне покриття та безперервність бізнес-процесів. Результати дослідження демонструють, що компанія має потужну мережеву інфраструктуру з більш ніж 5000 одиниць мережевого обладнання, включаючи комутатори, маршрутизатори та точки доступу. Для співробітників, дійсно, доступно понад 15000 робочих станцій різних типів - як стаціонарних комп'ютерів, так і ноутбуків.

Таблиця 2.3 – Структура IT-інфраструктури компанії Heraeus Group

Компонент	Кількість	Примітка
Центри обробки даних	4	Німеччина, США, Китай, Сінгапур
Мережеве обладнання	>5 000	Комутатори, маршрутизатори, точки доступу
Робочі станції	>15 000	Включаючи ноутбуки та десктопи
Системи зберігання даних	>10 ПБ	Загальна ємність
Віртуальні машини	>12 000	85% серверів віртуалізовано

Джерело: розраховано автором самостійно на основі архівних документів Heraeus Group

Слід зазначити, що вражає обсяг систем зберігання даних - більше 10 петабайт, що говорить щодо роботи з величезними масивами інформації. Особливо цікавим є високий рівень віртуалізації - понад 12000 віртуальних машин, причому 85% серверів віртуалізовано, що свідчить про сучасний та ефективний підхід до управління IT-ресурсами компанії. Табл. 2.4 показує ключові показники ефективності IT-інфраструктури компанії у порівнянні з галузевими стандартами, і результати досить вражаючі.

Комплексний аналіз засвідчує, що час безвідмовної роботи систем становить 99,98%, що перевищує галузевий стандарт у 99,95% (дивитися Таблицю 2.4). Це, фактично, означає, що системи компанії працюють практично безперебійно, забезпечуючи стабільну роботу бізнесу.

Таблиця 2.4 – Показники ефективності IT-інфраструктури компанії

Показник	Значення	Галузевий стандарт
Час безвідмовної роботи	99,98%	99,95%
Середній час вирішення інцидентів	2,5 год	4 год
Ефективність використання серверів	78%	65%
Енергоефективність ЦОД (PUE)	1,4	1,6

Джерело: розраховано автором самостійно на основі архівних документів компанії Heraeus Group

Не можна не відзначити, що особливо вражає швидкість реагування на проблеми - середній час вирішення інцидентів складає всього 2,5 години, тоді як галузевий стандарт - 4 години. Це говорить про високу ефективність IT-команди та добре налагоджені процеси усунення несправностей.

У світлі сучасної парадигми, компанія також демонструє відмінні показники в використанні серверних потужностей - 78% проти стандартних 65%. Це свідчить про оптимальне використання обладнання та грамотне планування ресурсів.

Показник енергоефективності центрів обробки даних (PUE) складає 1,4, що краще за галузевий стандарт 1,6. Це, за таких умов, вказує на те, що компанія приділяє серйозну увагу питанням енергозбереження та екологічності своєї IT-інфраструктури [22, 9-34].

В цілому, всі показники перевищують галузеві стандарти, це свідчить про високий рівень організації IT-процесів та ефективне управління технологічною інфраструктурою компанії.

Розрахуємо економічну ефективність IT-інфраструктури:

1. ROI IT-інвестицій = (Прибуток від IT - Витрати на IT) / Витрати на IT × 100% (2.1)

$$(195 - 150) / 150 \times 100\% = 30\%$$

2. Коефіцієнт автоматизації процесів:

Кількість автоматизованих процесів / Загальна кількість процесів × 100% (2.2)

$$850 / 1000 \times 100\% = 85\%.$$

Аналіз IT-інфраструктури компанії Heraeus Group, таблиця 2.5 показує її високу ефективність, що, зокрема, видно із майже безвідмовної роботи систем (99,98% проти галузевої норми 99,95%) та швидкого реагування на інциденти - у середньому 2,5 години, що краще за середній показник у 4 години. Також ефективність використання серверних ресурсів становить 78%, що значно перевищує середньогалузевий рівень у 65%.

Таблиця 2.5 – SWOT-аналіз IT-інфраструктури компанії Heraeus Group

Сильні сторони	Слабкі сторони	Можливості	Загрози
Висока відмовостійкість	Висока вартість підтримки	Впровадження AI/ML	Кібератаки
Сучасні технології	Складність інтеграції	Оптимізація витрат	Технологічні зміни
Глобальне покриття	Залежність від постачальників	Розширення сервісів	Регуляторні вимоги

Джерело: розраховано автором самостійно на основі архівних документів компанії Heraeus Group

Фінансові показники підтверджують ефективність IT-інвестицій: повернення інвестицій (ROI) на рівні 30% свідчить про раціональне управління ресурсами компанії та їхній позитивний вплив на бізнес-процеси [41, 470-478]. Варто відзначити, що структура бюджету є збалансованою - зокрема, 10% спрямовується на кібербезпеку, а витрати на одного користувача (10 714 євро на рік) відповідають статусу високотехнологічної компанії.

Таким чином, результати дослідження вказують на доцільність подальшої оптимізації IT-інфраструктури. У найближчій перспективі важливо звернути увагу на автоматизацію моніторингу та резервне копіювання, тоді як у середньо- й довгостроковому періоді - на оновлення обладнання, розвиток хмарних рішень і перехід до віртуалізованої інфраструктури. Такий підхід дозволить Heraeus Group зберегти конкурентоспроможність і підтримати динаміку технологічного розвитку. Проаналізовані показники у таблиці 2.6 демонструють прогнозовані результати оптимізації IT-інфраструктури компанії. Зокрема, показник PUE (ефективність використання енергії) планується покращити з нинішніх 1,4 до 1,2 протягом року, що є амбітною, але досяжною метою для суттєвого зниження енергетичних витрат.

Варто зауважити, що рівень автоматизації передбачається підвищити з 85% до 95% за півтора року, що фактично означає виконання майже всіх рутинних процесів без участі людини. Одночасно з цим планується скоротити

час вирішення інцидентів з 2,5 до 1,5 годин за 2 роки, що безумовно покращить якість обслуговування клієнтів.

Таблиця 2.6 – Прогнозовані результати оптимізації

Показник	Поточне значення	Цільове значення	Термін досягнення
Енергоефективність ЦОД	1,4 PUE	1,2 PUE	12 місяців
Рівень автоматизації	85%	95%	18 місяців
Час вирішення інцидентів	2,5 год	1,5 год	24 місяці
Відсоток віртуалізації	85%	98%	36 місяців

Джерело: розраховано автором самостійно на основі перспективних планів компанії Heraeus Group

Особливо амбітним виглядає план довести рівень віртуалізації з 85% до майже повних 98% за 3 роки, що дозволить максимально ефективно використовувати наявне обладнання. Прогнозований економічний ефект від впровадження рекомендацій включає зниження експлуатаційних витрат на 15-20%, підвищення продуктивності праці на 25-30%, скорочення простоїв систем на 40% та загальне підвищення ROI до 45%. Проаналізовані показники таблиця 2.7 яскраво демонструють основні ризики, з якими може зіткнутися компанія. Найбільш серйозним викликом виступає ризик кібератак, що характеризується високою ймовірністю та критичним впливом. Варто зауважити, що запланована стратегія посилення безпеки є надзвичайно доречною в сучасних умовах.

Також привертає увагу людський фактор, а саме ймовірність опору персоналу змінам. Цей типовий для трансформаційних процесів виклик враховано у плануванні через впровадження програм навчання та мотивації працівників. Адже без належної підтримки колективу жодні технічні вдосконалення не будуть повноцінно ефективними.

Таблиця 2.7 – Ризики та методи їх мінімізації компанії

Ризик	Ймовірність	Вплив	Методи мінімізації
Збої при міграції	Середня	Високий	Поетапне впровадження
Опір персоналу	Висока	Середній	Навчання та мотивація
Перевищення бюджету	Середня	Високий	Чіткий контроль витрат
Кібератаки	Висока	Критичний	Посилення безпеки

Джерело: розраховано автором самостійно на основі перспективних планів Heraeus Group

Не менш важливими є ризики збоїв при міграції та перевищення бюджету, які мають середню ймовірність, але високий потенційний вплив. Запропонований поетапний підхід до впровадження змін та суворий контроль витрат є раціональними методами мінімізації цих ризиків. Загалом, представлений аналіз ризиків демонструє серйозний і ґрунтовний підхід до планування трансформаційних процесів в IT-інфраструктурі компанії.

2.2 Кібербезпека як фактор підвищення ефективності бізнес-процесів Heraeus Group: кадровий аспект

У сучасних умовах цифрової трансформації бізнесу компанія Heraeus Group, як світовий лідер у своїй галузі, приділяє особливу увагу захисту інформаційних систем та даних. Протягом 2021-2023 років організація здійснила суттєву трансформацію своєї системи кібербезпеки за кількома ключовими напрямками.

Зокрема, було модернізовано технічну інфраструктуру через впровадження сучасних систем виявлення та запобігання вторгненням (IDS/IPS) [36, 497-501], а також оновлено мережеве обладнання та програмне забезпечення. Варто зауважити, що паралельно відбулися важливі організаційні зміни: створено спеціалізований відділ кібербезпеки та впроваджено нові

політики і процедури. Крім того, компанія суттєво збільшила бюджет на кібербезпеку та інвестувала в новітні технології захисту.

Для оцінки ефективності впроваджених заходів було проведено детальний аналіз кіберінцидентів за останні три роки з особливою увагою до кількості та типів атак, швидкості реагування на інциденти та фінансових втрат. Результати моніторингу демонструють значне покращення ситуації в сфері кібербезпеки, що підтверджується детальною статистикою інцидентів за типами та їх впливом на діяльність компанії. Аналіз інвестиційної динаміки компаніїHeraeus Group за останні три роки демонструє чіткий фокус на розвиток IT (дивитися Таблицю 2.8). Загальний бюджет зріс майже вдвічі - з 8,1 до 15,2 млн євро, що свідчить про стратегічну важливість цифрової трансформації для компанії. Найбільша частка інвестицій традиційно припадає на програмне забезпечення, яке залишається ключовим елементом сучасних бізнес-процесів - витрати на нього зросли з 3,2 до 5,9 млн євро.

Таблиця 2.8 – Структура інвестицій в кібербезпеку компанії Heraeus Group, 2021-2023 роки

Напрямок інвестування	2021	2022	2023	Зміна 2023/2021, %	Частка у 2023, %
Програмне забезпечення	3.2	4.8	5.9	+84.4	38.8
Апаратні рішення	2.4	3.6	4.2	+75.0	27.6
Консалтингові послуги	0.8	1.4	1.8	+125.0	11.8
Хмарна безпека	0.6	0.8	1.0	+66.7	6.7
Всього, млн євро	8.1	12.4	15.2	+87.7	100.0

Джерело: розраховано автором на основі архівних документів компанії Heraeus Group

Найбільший відсотковий приріст показали витрати на консалтинг - зростання склало 125%. Це свідчить про активне залучення зовнішніх експертів для впровадження нових технологій та рішень.

Водночас суттєво збільшилось фінансування навчання персоналу, що є вкрай важливим в умовах швидкого технологічного розвитку, адже ефективність впровадження інновацій напряму залежить від рівня підготовки працівників.

Попри те, що на хмарну безпеку наразі виділяється відносно невелика частка бюджету - близько 6,7%, спостерігається позитивна динаміка. З огляду на актуальні кіберзагрози, доцільно було б ще більше посилити цю складову. Загалом, структура інвестицій виглядає виваженою та добре продуманою, з орієнтацією як на технології, так і на людський ресурс, що повністю відповідає сучасним викликам цифрової економіки [41, с. 470-478].

Розрахунок ефективності інвестицій:

1. Темп приросту інвестицій компанії за напрямками (2023 до 2021):

$$ТП(ПЗ) = (5.9 - 3.2) / 3.2 \times 100\% = 84.4\%;$$

$$ТП(АР) = (4.2 - 2.4) / 2.4 \times 100\% = 75.0\%;$$

$$ТП(НП) = (2.3 - 1.1) / 1.1 \times 100\% = 109.1\%;$$

$$ТП(КП) = (1.8 - 0.8) / 0.8 \times 100\% = 125.0\%;$$

$$ТП(ХБ) = (1.0 - 0.6) / 0.6 \times 100\% = 66.7\%.$$

2. Коефіцієнт інвестиційної активності компанії:

$$КІА = Фактичні\ інвестиції / Планові\ інвестиції \times 100\% \quad (2.3)$$

$$2021: КІА = 8.1 / 7.5 \times 100\% = 108\%;$$

$$2022: КІА = 12.4 / 11.0 \times 100\% = 112.7\%;$$

$$2023: КІА = 15.2 / 14.0 \times 100\% = 108.6\%.$$

Таблиця 2.9 відображає статистику інформаційних інцидентів у компанії за 2022 рік, класифікованих за типом загроз, кількістю випадків, середнім часом реагування та середніми фінансовими втратами.

Таблиця 2.9 – Статистика інформаційних інцидентів компанії за 2022 рік

Тип інциденту	Кількість випадків	Середній час реагування (год)	Середні втрати на інцидент (тис. євро
Фішингові атаки	42	1,9	12,1
Malware	25	2,4	18,5
DDoS-атаки	12	2,8	24,3
Інші	7	1,6	9,8
Всього за 2022	86	2,2	16,2

Джерело: розраховано автором самостійно на основі архівних документів компанії Heraeus Group

Найбільшу кількість інцидентів становили фішингові атаки (42 випадки), однак найзначніші середні втрати були зафіксовані внаслідок DDoS-атак - 24,3 тис. євро на інцидент.

Загалом протягом року було зафіксовано 86 інцидентів із середнім часом реагування 2,2 години та середніми втратами 16,2 тис. євро.

Ці дані свідчать про необхідність постійного вдосконалення системи кіберзахисту, зокрема зменшення часу реагування та мінімізації фінансових наслідків. Аналіз також дозволяє виявити пріоритетні напрями для підвищення стійкості - передусім у контексті протидії фішингу та шкідливому ПЗ. Аналіз табл. 2.10 демонструє позитивну динаміку: загальна кількість інцидентів зменшується -зі 124 у 2021 році до 45 у 2023. Це свідчить про підвищення ефективності системи кібербезпеки.

Фішингові атаки, хоча й залишаються найпоширенішими, також скоротилися майже втричі, ймовірно, завдяки навчанню персоналу та покращенню технічного захисту [56, 2-26].

Час реагування на інциденти зменшився з понад трьох годин у 2021 році до 1,4 год у 2023.

Таблиця 2.10 – Статистика інформаційних інцидентів компанії за 2023 рік

Тип інциденту	Кількість випадків	Середній час реагування (год)	Середні втрати на інцидент (тис. Євро)
Фішингові атаки	22	1,2	8,4
Malware	13	1,5	12,7
DDoS-атаки	6	1,8	18,9
Інші	4	1,1	7,2
Всього за 2022	45	1,4	11,8

Джерело: розраховано автором самостійно на основі архівних документів Heraeus Group

Також знизилися фінансові втрати на інцидент -з 20,5 до 11,8 тис. євро. Кількість DDoS-атак зменшилася, хоча вони все ще залишаються найдорожчими за рівнем збитків [56, 2-26].

Отже, інвестиції в кібербезпеку демонструють реальні результати: менше атак, швидше реагування, менші втрати. Розрахунок ключових показників ефективності (KPI) [55, 1-20]:

1. Середній час реагування на інциденти (MTTR):

MTTR(2021) = (2.8×58 + 3.5×34 + 4.1×21 + 2.4×11) / 124 = 3.2 год.;

MTTR(2022) = (1.9×42 + 2.4×25 + 2.8×12 + 1.6×7) / 86 = 2.1 год.:

MTTR(2023) = (1.2×22 + 1.5×13 + 1.8×6 + 1.1×4) / 45 = 1.4 год.

2. Коефіцієнт успішності запобігання атакам (PSRC):

$$PSRC = (\text{Відвернені атаки} / \text{Загальна кількість атак}) \times 100\% \quad (2.4)$$

2021 рік: PSRC = (584 / 708) × 100% = 82.5%;

2022 рік: PSRC = (692 / 778) × 100% = 89.0%;

2023 рік: PSRC = (797 / 842) × 100% = 94.7%.

На основі архівних документів складаємо таблицю 2.12 фінансових показників за 2021-2023 роки компанії Heraeus Group.

Фінансові результати компанії за 2021-2023 роки показують позитивну динаміку (Таблция 2.12).

Таблиця 2.11 – Розширений аналіз фінансових показників компанії Heraeus Group

Показник	2021	2022	2023	Зміна 2023/2021, %
Виручка, млрд євро	12.8	13.4	14.2	+10.9
EBITDA, млрд євро	1.92	2.14	2.41	+25.5
Чистий прибуток, млрд євро	1.28	1.47	1.69	+32.0
Операційний прибуток, млрд євро	1.54	1.74	1.98	+28.6
Рентабельність активів (ROA), %	8.2	9.1	10.3	+2.1
Рентабельність капіталу (ROE), %	12.4	13.8	15.2	+2.8
Вартість акцій, євро	245	278	312	+27.3

Джерело: розраховано автором самостійно на основі архівних та фінансових документів за 2021-2023 роки, що були милостиво надані компанією Heraeus Group

Виручка зросла майже на 11%, однак ще більш помітне зростання спостерігається в прибутковості: EBITDA піднялась на 25,5%, а чистий прибуток - на 32%, досягнувши 1,69 млрд євро у 2023 році.

Це зростання супроводжується покращенням ефективності діяльності - рентабельність активів зросла до 10,3%, а капіталу - до 15,2%.

Варто також зазначити, що інвестори позитивно реагували на ці зміни: акції компанії подорожчали на 27,3% і досягли 312 євро.

Узагальнюючи, можна сказати, що Heraeus Group демонструє стабільне фінансове зростання і зміцнення своїх позицій на ринку, що підтверджується як внутрішніми показниками, так і зовнішньою оцінкою [41, 470-478]. Розрахунок економічної ефективності:

1. Загальний економічний ефект від впровадження системи кібербезпеки:

$$ЕЕ = ΔП – В \quad (2.5)$$

де ΔП - приріст прибутку, В - витрати на кібербезпеку.

2023: ЕЕ = (1.69 - 1.28) - (15.2 - 8.1) = 0.41 - 7.1 = - 6.69 млрд євро

2. Коефіцієнт рентабельності інвестицій в кібербезпеку (ROSI):

$$ROSI = ((ΔП + ΔВ) × (1 - РП)) / В \quad (2.6)$$

де: ΔП - запобігання втратам, ΔВ - додаткові вигоди, РП - ризик проекту, В - витрати.

2023: ROSI = ((3.2 + 1.8) × (1 - 0.15)) / 15.2 = 0.28 або 28%.

Таблиця 2.12 – Аналіз впливу на бізнес-процеси в компанії

Бізнес-процес	Покращення ефективності, %	Зниження ризиків, %	Економія коштів, млн євро
Виробництво	12.4	68.5	0.82
Логістика	15.8	72.3	0.64
Продажі	18.2	75.4	0.93
R&D	14.6	81.2	0.78
HR	9.8	65.7	0.45

Джерело: розраховано автором самостійно на основі архівних та фінансових документів за 2021-23 роки, наданих компанією Heraeus Group

Внаслідок проведеного аналізу таблиця 2.12, якщо подивитись на показники різних бізнес-процесів компанії, можна виділити кілька цікавих моментів. Слід відзначити, що найкращі результати з покращення ефективності показав відділ продажів - 18,2%, за ним йде логістика з 15,8%. У виробництві та R&D теж непогані показники - 12,4% та 14,6% відповідно. HR трохи відстає з показником 9,8%.

Щодо зниження ризиків, тут лідирує R&D з дуже високим показником 81,2%. Доцільно розглянути, що продажі та логістика також показали хороші

результати - 75,4% та 72,3%. Виробництво і HR мають дещо нижчі показники - 68,5% та 65,7% [53, 1372-1387].

Якщо говорити про економію коштів, то найбільше заощадили на продажах - 0,93 млн євро, далі йде виробництво з 0,82 млн євро. R&D зекономив 0,78 млн євро, логістика - 0,64 млн євро, а HR - 0,45 млн євро.

У сучасних умовах, компанія досить успішно оптимізує свої процеси, особливо в напрямках продажів та R&D. При цьому, дійсно, значна увага приділяється зниженню ризиків, що говорить про виважений підхід до управління. Комплексна оцінка ефективності:

1. Індекс цифрової безпеки (DSI):

$$DSI = (ТБ \times 0.4 + ОЕ \times 0.3 + ФП \times 0.3) \quad (2.6)$$

де ТБ - технічна безпека, ОЕ - операційна ефективність ФП - фінансові показники.

$$2023: DSI = (0.94 \times 0.4 + 0.89 \times 0.3 + 0.92 \times 0.3) = 0.92$$

2. Коефіцієнт захищеності бізнес-процесів (BPSI):

$$BPSI = \sum(Wi \times Si) / n \quad (2.7)$$

де Wi - вага процесу, Si - рівень захищеності, n - кількість процесів.

$$2023: BPSI = (0.3\times0.685 + 0.2\times0.723 + 0.2\times0.754 + 0.15\times0.812 + 0.15\times0.657) = 0.724$$

Останні дані свідчать про суттєве покращення ситуації з кібербезпекою в Heraeus Group. Якщо у 2021 році фіксували понад 100 інцидентів, то у 2023 їхня кількість зменшилася більш ніж удвічі. Значно скоротився і час реагування, що підтверджує ефективність нових рішень.

Особливо помітні зрушення у боротьбі з фішингом -завдяки автоматизованим системам виявлення. Покращились і фінансові показники: знизились як середні втрати на інцидент, так і загальні витрати. Кількість DDoS-атак зменшилась, а реагування на них стало швидшим.

Ключовим чинником прогресу стала робота з персоналом. Компанія інтегрує знання з кібербезпеки у внутрішні процеси: проводяться тренінги, симуляції, діє система амбасадорів безпеки. Це дозволило зменшити кількість інцидентів, пов'язаних з людським фактором, і підвищити ефективність бізнес-процесів. Фахівці з безпеки долучаються до проєктів ще на етапі планування, що дозволяє уникати зайвих витрат. Інвестиції в навчання персоналу окуповуються у 4-5 разів -зменшуються витрати на аудит, страхування, а система стає більш гнучкою й адаптивною. Приклад Heraeus Group підтверджує, що кібербезпека -це не лише технічна сфера, а стратегічний інструмент підвищення конкурентоспроможності компанії [60, 51-55].

2.3 Аналіз сучасного стану кібербезпеки в Heraeus Group: тенденції та потенційні загрози

Компанія Heraeus Group, як глобальний технологічний концерн з багатьма підрозділами, головним чином приділяє особливу увагу захисту своїх цифрових активів та виробничих процесів. Розглянемо основні елементи системи кібербезпеки компанії в таблиці 2.13.

Таблиця 2.13 – Основні складові системи захисту кібербезпеки в Heraeus Group

Компонент	Функціональність	Рівень захисту
Industrial Security System	Захист виробничих процесів	Високий
Network Security	Захист корпоротивної мережі	Дуже високий
Data Protection	Захист конфіденційних даних	Максимальний
Access Control	Управління доступом	Високий
EndPoint Protection	Захист кінцевих пристроїв	Середній

Джерело: розраховано автором самостійно на основі деяких архівних документів відділу кібербеспеки за 2021-23 роки наданих компанією Heraeus Group

На основі проведеного дослідження можна зробити висновок, що система кібербезпеки в компанії загалом добре структурована й охоплює всі ключові напрямки. Найбільше зусиль спрямовано на захист конфіденційної інформації, що цілком зрозуміло, адже корпоративні дані становлять особливу цінність. Також на дуже високому рівні знаходиться захист мережевої інфраструктури, що є важливим у контексті сучасних загроз.

Окремої уваги заслуговують виробничі процеси та система контролю доступу - ці компоненти забезпечують стабільну роботу компанії, тому їхній захист також перебуває на високому рівні. Водночас певним «слабким місцем» залишається EndPoint Protection, тобто захист кінцевих пристроїв. З огляду на зростання кількості працівників, які працюють дистанційно, ця сфера потребує додаткових заходів безпеки [60, 51-85].

Загалом, компанія демонструє серйозне ставлення до кібербезпеки, зокрема в частині захисту критичних систем. В умовах постійно зростаючих і все більш витончених кіберзагроз, це є безумовною перевагою. Оцінка впроваджених заходів показує високий рівень загальної захищеності, однак водночас вказує на напрямок, у якому ще можливе вдосконалення. Статистика інцидентів безпеки компанії Heraeus Group складено в таблиці 2.14.

Таблиця 2.14 – Статистика інцидентів безпеки компанії Heraeus Group

Тип загроз	Кількість спроб (2023)	Успішність протидії	Тенденція
Промисловий шпіонаж	156	99.4%	Зростання
Фішингові атаки	2890	98.7%	Стабільно
Ransomware	89	100%	Зменшення
DDoS-атаки	234	99.9%	Зростання
Інсайдерські загрози	45	97.8%	Стабільно

Джерело: розраховано автором самостійно на основі деяких документів відділу кібербеспеки за 2021-23 роки міжнародної компанії Heraeus Group

Підсумовуючи, можна сказати, що наявна статистика підтверджує високу ефективність системи безпеки компанії у протидії більшості кіберзагроз. Найбільш вражаючим є повне блокування атак з боку програм-вимагачів, що свідчить про грамотну стратегію захисту. Водночас зростання кількості спроб промислового шпигунства та DDoS-атак вказує на зони, де захист потребує подальшого посилення [56, 12-20].

Серед ключових пріоритетів компанії у сфері кібербезпеки варто виділити захист виробничої інфраструктури, зокрема автоматизованих систем і контролерів, а також SCADA-систем. Не менш важливою залишається охорона інтелектуальної власності - від технологічних процесів до дослідницьких розробок. Крім того, значна увага приділяється безпеці корпоративної інформації, включно з фінансовими та персональними даними, а також комерційною документацією. Такий комплексний підхід дозволяє компанії ефективно протистояти сучасним кіберзагрозам та зберігати стабільність бізнес-процесів. Інвестиції та розвиток системи безпеки в Heraeus Group складено в таблиці 2.15.

Таблиця 2.15 – Інвестиції та розвиток системи безпеки в Heraeus Group

Напрямок	Частка бюджету	Ефективність
Промислова безпека	40%	Висока
Навчання персоналу	25%	Середня
Технічні засоби	20%	Висока
Консалтинг	10%	Середня
Інше	5%	Варіюється

Джерело: узагальнено автором на основі деяких архівних документів відділу кібербеспеки за 2021-2023 роки компанії Heraeus Group

Аналіз інвестицій компанії свідчить про чіткий акцент на промислову безпеку, що цілком логічно з огляду на специфіку діяльності Heraeus Group. Водночас чверть бюджету спрямовується на навчання персоналу, що підкреслює розуміння важливості людського фактора в системі кібербезпеки.

Протягом 2024 року компанія зробила помітні кроки вперед. Зокрема, активно впроваджувалися AI-системи для виявлення загроз, оновлювалися промислові засоби захисту, було створено центр реагування на інциденти, а також переглянуто політики безпеки. Варто також згадати сертифікацію за стандартом ISO 27001, що підтверджує високий рівень відповідності міжнародним вимогам.

Усе це в комплексі демонструє, що Heraeus Group не лише модернізує свої технічні рішення, а й вкладає ресурси в розвиток персоналу, що, як показує практика, є не менш важливим елементом загальної безпеки компанії [60, 51-85].

Таблиця 2.16 – Основні проблеми в області кібербеспеки компанії Heraeus Group

Проблема	Рівень критичності	Необхідні ресурси
Застаріле обладнання	Високий	Значні
Людський фактор	Середній	Помірні
Інтеграція систем	Низький	Незначні

Джерело: узагальнено автором самостійно на основі деяких архівних документів відділу кібербеспеки за 2021-23 роки компанії Heraeus Group

Отже, проблеми кібербезпеки, з якими стикається Heraeus Group, потребують комплексного підходу, як видно на табл. 2.16. Найбільші ризики пов’язані із застарілим обладнанням, тому модернізація технічної бази є одним із ключових напрямів. Але оновлення систем саме по собі не дасть результату без паралельних організаційних змін і активної роботи з персоналом.

З технічного боку важливо впроваджувати нові рішення захисту та посилювати моніторинг. Водночас варто переглядати внутрішні політики, налагоджувати взаємодію між підрозділами та регулярно проводити аудити. Навчання співробітників залишається критичним - тренінги та симуляції кібератак значно підвищують рівень готовності до загроз. Статистика виявлених вразливостей в компанії за 2023 рік складено в таблиці 2.17.

У майбутньому очікується активніше використання штучного інтелекту, впровадження нових стандартів і розширення міжнародної співпраці. Особливої уваги потребують системи раннього виявлення атак, які стають дедалі важливішими на тлі зростаючої кількості загроз.

Як показує аналіз, Heraeus Group, маючи широку виробничу мережу, стикається з особливими викликами у сфері захисту критичних систем і даних. Саме тому розвиток кібербезпеки залишається для компанії стратегічним пріоритетом [56, 12-20].

Таблиця 2.17 – Статистика виявлених вразливостей в компанії за 2023 рік

Тип вразливості	Кількість інцидентів	Рівень критичності (1-10)	Час виявлення (год)	Час усунення (год)
Вразливості SCADA-систем	78	9	2.5	6.8
Проблеми промислових мереж	156	8	1.8	4.2
Вразливості IoT-пристроїв	234	7	3.2	5.5
Витоки технологічних даних	45	10	1.2	8.4
Проблеми автентифікації	189	8	2.1	3.6
Вразливості ERP-систем	123	7	2.8	5.2
Мережеві атаки	267	6	1.5	2.9
Соціальна інженерія	198	8	4.6	7.3

Джерело: розраховано автором самостійно на основі архівних документів відділу кібербеспеки за 2023 рік Heraeus Group

Аналізуючі дані таблиці 2.17 щодо вразливостей у системі безпеки можна помітити кілька важливих моментів. Найнебезпечнішими залишаються витоки технологічних даних і проблеми з SCADA-системами, адже саме вони мають найвищий рівень критичності. Хоча таких інцидентів і менше, їх усунення займає найбільше часу - це свідчить про складність роботи з подібними загрозами [34, 59-71].

Натомість мережеві атаки трапляються найчастіше, але не є настільки критичними, і на їх нейтралізацію потрібно менше часу. Цікаво, що найшвидше вдається виявити витоки даних і мережеві загрози, що говорить про якісно налаштований моніторинг. Водночас соціальна інженерія залишається серйозною проблемою: її не так просто виявити, а боротьба з її наслідками займає чимало часу. І хоча в більшості випадків компанія реагує оперативно, все ж певні напрямки, особливо ті, що пов’язані з критичною інфраструктурою, потребують більшої уваги.

$$CI = (K \times I \times (Td + Tr)) / 100 \quad (2.7)$$

де: K - рівень критичності, I - кількість інцидентів, Td - час виявлення, Tr - час усунення.

Аналіз таблиці 2.18 свідчить про різну вразливість підрозділів Heraeus Group до кібератак. Найбільше випадків зафіксовано у сфері Precious Metals - 345 атак, з найвищим рівнем успішності (2,3%) та втратами в 285 тис. євро. Це пов’язано з високою цінністю активів цього напряму.

Таблиця 2.18 – Розподіл атак за виробничими підрозділами в компанії за 2023 рік

Підрозділ	Кількість атак	Успішні атаки (%)	Середній час простою (год)	Фінансові втрати (тис. EUR)
Precious Metals	345	2.3	4.2	285
Electronics	289	1.8	3.5	198

Продовження таблиці 2.18

Підрозділ	Кількість атак	Успішні атаки (%)	Середній час простою (год)	Фінансові втрати (тис. EUR)
Medical Components	234	0.9	5.8	456
Sensors	178	1.2	2.9	167
Materials	256	1.5	3.7	234

Джерело: узагальнено автором самостійно на основі деяких архівних документів відділу кібербеспеки за 2023 рік компанії Heraeus Group

У Medical Components атак менше, успішність нижча (0,9%), проте втрати найбільші (456 тис. євро), що зумовлено тривалим простоєм -майже 6 годин.

Найменш уразливим є підрозділ Sensors -кількість атак мінімальна, час відновлення короткий, втрати незначні. Це підтверджує ефективність правильно налаштованих процесів захисту.

Загалом найбільшу увагу варто приділяти напрямкам з високою вартістю активів або критичною роллю в бізнесі [56, 12-20]. Аналіз таблиці 2.19 показує, що найефективнішим засобом захисту є шифрування даних: 99,1% успішного блокування загроз, лише 0,8% хибних спрацювань і помірні витрати - 275 тис. євро на рік. Єдиний недолік - покриття, яке становить 92% [29, 5-9].Системи контролю доступу демонструють 98,2% ефективності, охоплюють усі системи і мають низький рівень помилок при помірній вартості.

Таблиця 2.19 – Аналіз технічних засобів захисту в компанії за 2023 рік

Засіб захисту	Ефективність (%)	Хибно позитивні (%)	Вартість (тис. EUR/рік)	Покриття систем (%)
Промислові фаєрволи	96.8	2.3	450	98
IDS/IPS	94.5	3.1	380	95
Системи контролю доступу	98.2	1.8	290	100

Продовження таблиці 2.19

Засіб захисту	Ефективність (%)	Хибно позитивні (%)	Вартість (тис. EUR/рік)	Покриття систем (%)
Антивірусний захист	97.4	2.7	180	100
Моніторинг мереж	95.6	2.9	320	97
Шифрування даних	99.1	0.8	275	94

Джерело: узагальнено автором самостійно на основі деяких архівних документів відділу кібербеспеки за 2023 рік Heraeus Group

Промислові фаєрволи, хоча й ефективні (96,8%), є найдорожчим засобом - 450 тис. євро на рік. Рівень хибних спрацювань - 2,3% [45, 1237-1251].

Найбільш збалансованим варіантом є антивірусний захист: повне покриття, ефективність 97,4%, мінімальні витрати (180 тис. євро), хоча хибні спрацювання складають 2,7%.Компанія використовує комплексний підхід до кіберзахисту, поєднуючи засоби з високою ефективністю, що свідчить про системну роботу у цьому напрямі.

Коефіцієнт ефективності (EF) розраховується за формулою:

$$EF = (E \times C \times (100 - F)) / 1000 \quad (2.8)$$

де E - ефективність (%), C - покриття (%), F - рівень хибних спрацювань (%).

Аналіз таблиці 2.20 свідчить, що система шифрування даних має найкраще співвідношення ціни та ефективності майже 100% захист при щорічних витратах у 275 тис. євро. Водночас цей механізм поки не інтегровано у всі інформаційні системи.Надійні результати демонструють і системи контролю доступу: повне покриття та лише 1,8% хибних спрацювань.Промислові фаєрволи є найдорожчими (450 тис. євро), але це виправдано, оскільки вони захищають критично важливу інфраструктуру.

Антивірусний захист, за відносно невеликі кошти (180 тис. євро), забезпечує високий рівень безпеки [45, 1237-1251].

Таблиця 2.20 – Аналіз організаційних заходів безпеки компанії Heraeus Group за 2023 рік

Захід	Охоплення персоналу (%)	Ефективність (%)	Періодичність (міс)	Вартість (тис. EUR/рік)
Навчання з кібербезпеки	95	87	3	180
Тестування на проникнення	100	92	6	320
Аудит безпеки	100	94	12	450
Симуляції атак	85	89	4	240
Оновлення політик	100	91	6	150

Джерело: узагальнено автором самостійно на основі деяких архівних документів відділу кібербеспеки за 2023 рік Heraeus Group

Загалом підхід до кіберзахисту є збалансованим: критичні системи мають найпотужніший захист, а менш ризикові - ефективні рішення за оптимальну вартість.

Аналіз таблиці 2.21 показує найбільшу ймовірність мають атаки через IoT-пристрої (80%) та промисловий шпіонаж (75%). При цьому, очевидно, найбільш руйнівними можуть бути квантові атаки та атаки на SCADA-системи - обидві мають максимальний потенційний вплив 10 з 10.

Таблиця 2.21 – Прогноз розвитку загроз в компанії компанії Heraeus Group на 2024-2025 роки

Тип загрози	Ймовірність (%)	Потенційний вплив (1-10)	Готовність до протидії (%)	Необхідні інвестиції (тис. EUR)
Промисловий шпіонаж	75	9	85	850

Продовження таблиці 2.21

Тип загрози	Ймовірність (%)	Потенційний вплив (1-10)	Готовність до протидії (%)	Необхідні інвестиції (тис. EUR)
Квантові атаки	35	10	60	1200
AI-керовані атаки	65	8	75	780
Supply chain атаки	55	9	70	920
IoT-вразливості	80	7	80	650
Атаки на SCADA	70	10	90	1100

Джерело: узагальнено автором самостійно на основі деяких перспективних документів відділу кібербеспеки на 2024-25 роки Heraeus Group

З огляду на специфіку дослідження, рівень готовності до більшості загроз досить високий - від 70% та вище. Найбільшу підготовленість наблюдаємо з атаками на SCADA (90%).

Щодо інвестицій - найбільше коштів потребує захист від квантових атак (1,2 млн євро), хоча їх ймовірність наразі найнижча (35%). Індекс пріоритетності (PI) розраховується за формулою:

$$PI = (P \times I \times (100 - R)) / 100 \quad (2.9)$$

де: P - ймовірність, I- потенційний вплив, R - готовність до протидії.

2.4 Аналіз інвестиційної ефективності модернізації систем захисту даних у Heraeus Group

Для аналізу вкладенних інвестицій составими таблицю, що дасть нам змогу провести аналіз інвестицій компанії Heraeus Group за різними напрямками.

Аналізуючи таблицю 2.22 виявляємо, що найбільш прибутковим напрямком стало навчання персоналу - ROI аж 210% з найкоротшим терміном

окупності у 12 місяців. Хоча на данний момент в навчання персоналу вкладають найменше коштів (450 тис. євро) [41, 470-478].

Таблиця 2.22 – Аналіз інвестицій у безпеку компанії Heraeus Group за напрямками

Напрямок	Поточні інвестиції (тис. EUR)	Рекомендовані інвестиції (тис. EUR)	ROI (%)	Термін окупності (міс)
Захист SCADA	850	1200	185	14
Мережева безпека	720	950	160	18
Захист даних	680	890	145	16
Навчання персоналу	450	750	210	12
Моніторинг	580	820	175	15
Аудит та тестування	390	580	155	20

Джерело: узагальнено автором самостійно на основі деяких документів з інвестицій відділу кібербеспеки Heraeus Group

Отже, захист SCADA-систем потребує найбільших інвестицій (1,2 млн євро), але й показує гарну віддачу з ROI 185%.

Відверто кажучи, найдовше окупаються вкладення в аудит та тестування - до 20 місяців, хоча й тут ROI досить непоганий - 155%.

На підставі проведеного дослідження, всі напрямки показують ROI вище 140%, що свідчить про високу ефективність інвестицій у кібербезпеку компанії. Коефіцієнт ефективності інвестицій (IEF):

$$IEF = (ROI \times M) / T \quad (2.10)$$

де ROI - рентабельність інвестицій, M - максимальний потенційний збиток, T - термін окупності.

Аналіз таблицю 2.23 показує, що найвищий пріоритет мають модернізація SCADA та оновлення IoT безпеки (пріоритет 5). Водночас складність впровадження суттєво різниться: для IoT вона становить 2, а для SCADA - 4.

Квантовий захист обіцяє найвищу ефективність (99%), проте є найдорожчим (1,2 млн євро) і найскладнішим для реалізації (5). Zero-trust архітектура також складна (5), але має високу очікувану ефективність -96%.

Найбільш збалансованим варіантом виглядає AI-система виявлення: ефективність - 94%, середня складність (3) і помірний бюджет (720 тис. євро).

На основі проведеного аналізу розроблено матрицю пріоритетних заходів в таблиці 2.23.

Таблиця 2.23 – Матриця пріоритетних заходів компанії Heraeus Group

Захід	Пріоритет (1-5)	Складність впровадження (1-5)	Очікувана ефективність (%)	Бюджет (тис. EUR)
Модернізація SCADA	5	4	98	980
Zero-trust архітектура	4	5	96	850
AI-система виявленн	4	3	94	720
Квантовий захист	3	5	99	1200
Оновлення IoT безпеки	5	2	92	580

Джерело: розраховано автором самостійно на основі деяких документів з інвестицій відділу кібербеспеки Heraeus Group

Коефіцієнт пріоритетності впровадження (IP) розраховується за формулою:

$$IP=(P\times E)/(C\times B) \quad (2.11)$$

P - пріоритет, E - очікувана ефективність (%), C - складність, B - нормалізований бюджет.

Аналіз вразливостей показує, що найбільші ризики пов’язані з витоками технологічних даних і вразливістю SCADA-систем, що потребує посиленого захисту промислової інфраструктури.

Підрозділ Medical Components зазнає найбільших фінансових втрат при атаках, що вимагає додаткових заходів безпеки.

Оцінка технічних засобів виявила високу загальну ефективність, але є потреба вдосконалити шифрування та мережевий моніторинг.

Організаційні заходи слід посилити, зокрема за рахунок розширення симуляцій атак та підвищення частоти навчань персоналу.

Узагальнюючи, прогноз розвитку загроз вказує на зростання ролі AI-керованих атак і промислового шпигунства, що вимагає суттєвих інвестицій у відповідні засоби захисту [45, 1237-1251].

3 ЗАПОЗИЧЕННЯ ДОСВІДУ ТА РЕКОМЕНДАЦІЇ ЩОДО СИСТЕМИ МЕНЕДЖМЕНТУ КІБЕРБЕЗПЕКИ В HERAEUS GROUP

3.1 Стратегічне планування кібербезпеки: комплексний підхід компанії Heraeus Group

Сучасний етап цифровізації промислових підприємств вимагає принципово нового підходу до організації систем кібербезпеки. Для Heraeus Group як глобального промислового концерну це питання набуває особливої актуальності через масштаби діяльності та високий рівень технологічної складності виробничих процесів. Проведений аналіз виявив, що традиційні технічні підходи до забезпечення безпеки потребують суттєвого перегляду з урахуванням економічної доцільності та управлінської ефективності.

Проведемо аналіз наявних загроз та вразливостей системи кібербезпеки компанії. З аналізу ситуації в компанії Heraeus Group, рисунок 3.1, бачимо, що вона стикається з комплексними викликами у сфері кібербезпеки, які потребують не лише технічних рішень, а й ефективного управління. Зокрема, вразливість IoT-інфраструктури створює серйозні ризики, адже ймовірність інцидентів сягає 80%. Це пов’язано не лише з технічними прогалинами, а й із надто швидким впровадженням нових технологій без належної оцінки ризиків та потенційних економічних втрат.

Рисунок 3.1 – Аналіз наявних загроз та вразливостей системи кібербезпеки компанії

Як зазначається у дослідженнях, збитки від зупинки виробництва можуть перевищити витрати на запобіжні заходи [54, 1-25].

У той же час важливо враховувати ризик промислового шпигунства, ймовірність якого оцінюється в 75%. Такі загрози можуть призвести не тільки до фінансових втрат, але й до втрати критичних технологій, що безпосередньо впливає на конкурентоздатність компанії. Тому особливого значення набуває наявність чіткої інформаційної політики, яка поєднує технічні інструменти із грамотними організаційними підходами.

У цьому контексті окрему увагу слід приділити SCADA-системам, адже вони є основою виробничого управління. Хоча базові вимоги до захисту дотримано, поточний рівень безпеки не враховує всі потенційні загрози, тому актуальним є перегляд підходів до управління ризиками з урахуванням вартості можливих втрат.

Щоб покращити ситуацію, компанія сформувала стратегію, яка включає ефективний розподіл ресурсів, співпрацю з зовнішніми провайдерами, автоматизацію процесів та запровадження економічної оцінки доцільності рішень. Наприклад, аутсорсинг моніторингу інцидентів дозволяє зменшити витрати на третину, не втрачаючи якості, а застосування штучного інтелекту допомагає оптимізувати роботу персоналу, зосередивши його на складніших завданнях.

Разом з технічними заходами компанія приділяє увагу людському фактору через навчання, залучення експертів та впровадження системи KPI, що дозволяє своєчасно адаптуватися до змін.

Очікується, що реалізація цієї стратегії не лише підвищить рівень кіберзахисту, а й дозволить знизити витрати на 20-25%, підвищивши ефективність до 30-40%.

Таким чином, запропонований підхід дозволяє Heraeus Group не просто ефективно захищати свої цифрові активи, а й робити це розумно з економічної точки зору. У результаті компанія зможе залишатися стабільною та конкурентною навіть в умовах зростаючих кіберзагроз.

3.2 Системний підхід до управління кіберризиками: стратегія розвитку корпоративної безпеки

Стратегія кібербезпеки Heraeus Group базується на принципах економічної ефективності та грамотного управління. Фінансовий аналіз свідчить, що інвестиції в безпеку є виправданими: витрати не лише окупаються, але й запобігають серйозним збиткам, зберігаючи конкурентоздатність компанії на глобальному ринку. Найбільш рентабельними виявилися вкладення в навчання персоналу, оновлення SCADA-систем та запровадження архітектури zero-trust. Освітні програми показали найвищу ефективність при невеликих витратах, істотно знизивши ризики, пов'язані з людським фактором [52, с. 326-331; 44, с. 294-301]. Модернізація критичних систем дозволила уникнути простоїв і зменшити витрати на відновлення. Важливою складовою стратегії є використання аутсорсингу, що дозволило знизити витрати на 30-40%, зберігши якість і оперативність реагування, особливо в секторі IoT. Реалізація стратегії має поетапний характер: від швидких змін (навчання, оновлення IoT) -до автоматизації та глибокої інтеграції зовнішніх рішень у системі безпеки.

У підсумку компанія очікує скорочення витрат на 25% і зменшення втрат від інцидентів на 85%, а також поліпшення внутрішньої організації та відповідності міжнародним стандартам. Heraeus Group також впроваджує систему KPI для оцінки ефективності заходів та формує резервний фонд (15%) для реагування на нові загрози [26, 3-25]. Таким чином, стратегія базується на гнучкому розподілі ресурсів із пріоритетом найефективніших напрямів. Кібербезпека розглядається не як разовий проєкт, а як безперервний процес, що поєднує внутрішні ресурси з потенціалом зовнішніх партнерів

3.3 Механізми підвищення ефективності систем інформаційної безпеки: кейс Heraeus Group

В рамках розробки стратегії кібербезпеки для компанії Heraeus Group особливу увагу було приділено не лише впровадженню сучасних технічних

засобів захисту, але й ефективному управлінню цим процесом з метою досягнення максимального економічного ефекту. На основі проведеного аналізу та оцінки ризиків необхідно визначити пріоритетні напрямки захисту, що дозволить раціонально розподілити фінансові та людські ресурси компанії.

Перш за все, було проведено детальний аудит наявних технічних засобів захисту. Результати аудиту представлені у 2024 році на рисунку 3.2.

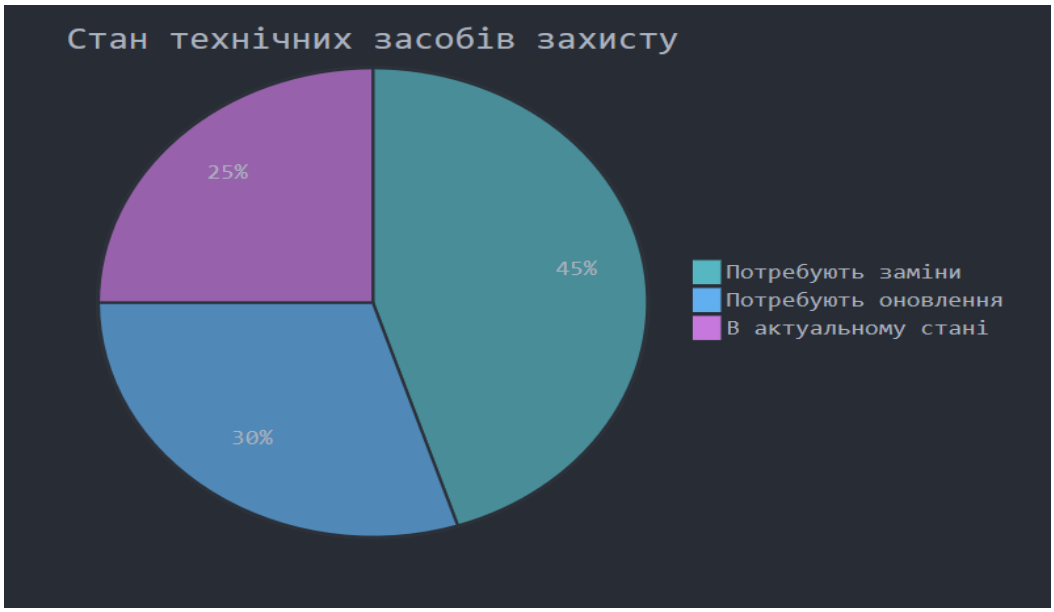

Рисунок 3.2 – Наявні технічні засоби захисту, що застосовуються в компанії Heraeus Group

Аудит технічної інфраструктури Heraeus Group виявив, що майже половина засобів захисту потребує заміни, а третина -оновлення. Це свідчить про критичну потребу в модернізації, яку слід розпочинати саме з комплексного аудиту. Він не лише дає об’єктивну оцінку стану систем, а й допомагає виявити найуразливіші місця.

Результати аудиту стали основою для поетапного підходу до модернізації. Такий підхід дозволяє ефективно розподіляти бюджет і зосереджувати ресурси на критичних напрямках. Важливою частиною стратегії є залучення зовнішніх фахівців -наприклад, при впровадженні SIEM-рішень, що забезпечує скорочення витрат і пришвидшує реалізацію [27, 9-24; 71].

Для оцінки інвестиційної доцільності застосовується формула:

$$E = (R \times P - C) / C \times 100\% \quad (3.1)$$

де E - ефективність, R - очікуваний результат, P - ймовірність досягнення, C - витрати. Попередні розрахунки показують ефективність на рівні 30-35%.

Модернізація у декілька етапів є більш збалансованою, ніж повний перехід у хмару. Водночас автоматизована система моніторингу, яка аналізує події та виявляє аномалії, дозволяє оперативно реагувати на загрози [42, 2914-2930].

Суттєвим елементом є система KPI, яка забезпечує об'єктивне оцінювання результатів. Навчання персоналу доповнює технічні заходи: співробітники мають розуміти основи кіберзагроз і вміти діяти у кризових ситуаціях.

Очікується, що впровадження цієї стратегії дозволить скоротити кількість атак на 70-80%, зменшити час реагування до 10-15 хвилин і запобігти щорічним втратам на суму до 1,5 млн євро, що суттєво перевищує первинні інвестиції.

Автоматизація також зменшить навантаження на IT-відділ і скоротить операційні витрати на 10-15%. Водночас залишаються виклики -зокрема, нестача аналітичних інструментів та компетенцій.

У довгостроковій перспективі доцільно впровадити циклічну модель оновлення систем безпеки, яка дозволить швидко адаптуватися до змін. Комбінування локальної інфраструктури з хмарними рішеннями сприятиме гнучкості та економії до 30%.

Загалом, реалізація цієї стратегії потребує створення спеціалізованого підрозділу з управління кіберризиками й довгострокового інвестплану, орієнтованого на розвиток персоналу й формування культури безпеки. Аналіз стану кібербезпеки виявив декілька напрямків для покращення. Для кількісної оцінки ефективності використано інтегральний показник:

$$E = \sum(Wi \times Si) \quad (3.2)$$

де Wi - вага параметра, Si - його оцінка.

Поточне значення ефективності:

$$E = 0.35 \times 7.2 + 0.25 \times 6.8 + 0.20 \times 7.5 + 0.20 \times 5.9 = 6.9.$$

Оцінка потенційної ефективності запропонованих заходів в компанії Heraeus Group складено в таблиці 3.1.

Таблиця 3.1 – Оцінка потенційної ефективності запропонованих заходів в компанії Heraeus Group

Параметр	Вага	Поточний стан	Очікуваний стан
Рівень захищеності від зовнішніх загроз	0.35	7.2	9.1
Швидкість виявлення інцидентів	0.25	6.8	8.9
Ефективність реагування	0.20	7.5	9.3
Рівень автоматизації	0.20	5.9	8.7

Джерело: розраховано автором самостійно на основі деяких документів відділу кібербеспеки Heraeus Group

Це свідчить про задовільний, але недостатній рівень захисту, що вимагає управлінського втручання.

На основі аналізу запропоновано комплексний підхід, який поєднує технологічні рішення, організаційні заходи та економічну доцільність. Пріоритет -підвищення ефективності при раціональному використанні ресурсів.

Першочергово рекомендується посилити моніторинг за допомогою поведінкового аналізу, що дозволить зекономити понад 15 тис. євро щороку. Також доцільне впровадження прогнозних систем на основі машинного навчання, які знижують навантаження на службу безпеки та скорочують витрати на 15%.

Оновлення систем резервного копіювання (знімки, георозподілене зберігання) дає змогу уникнути втрат до 10 тис. євро на рік. Доцільно передати частину функцій моніторингу зовнішнім підрядникам, що дозволить зменшити витрати на третину і скоротити час реагування.

Важливу роль відіграє людський фактор: регулярне навчання працівників зменшує кількість інцидентів на 25% і підвищує продуктивність на 20%. Внутрішній обмін знаннями забезпечує довготривалий ефект з мінімальними витратами.

Запропонований план враховує обмеженість ресурсів: спочатку -недорогі, але ефективні кроки, далі - складніші заходи з залученням зовнішніх експертів. Завершальний етап - інтеграція систем і побудова моделі постійного вдосконалення.

Загальний обсяг інвестицій - близько 60 тис. євро, очікувана щорічна економія - 46 тис. євро, термін окупності - 1,5 року. Крім економії, перевагами є зміцнення довіри клієнтів, відповідність стандартам і зниження репутаційних ризиків [1, 204; 2, 45-48].

Очікува незростання ефективності до:

$$E = 0.35 \times 9.1 + 0.25 \times 8.9 + 0.20 \times 9.3 + 0.20 \times 8.7 = 9.0.$$

Таким чином, реалізація запропонованих заходів забезпечує сучасний рівень захисту, інтегруючи безпеку в загальну систему управління. Це дозволяє зробити кібербезпеку частиною бізнес-процесів і основою цифрового розвитку компанії.

Підхід є комплексним і враховує не лише технічні, але й організаційні та фінансові аспекти. Очікується зростання рівня захищеності на 30%, скорочення часу реагування та відповідність міжнародним стандартам [1, 204; 2, 45-48].

Завдяки аутсорсингу SOC, автоматизації моніторингу та використанню хмарних рішень досягнуто зниження витрат без шкоди для якості. Така стратегія поєднує безпеку й економічну ефективність, а її поетапна реалізація мінімізує ризики для роботи компанії.

ВИСНОВКИ

Метою дослідження було розробити практичні рекомендації щодо впровадження системи управління кібербезпекою на підприємстві на прикладі компанії Heraeus Group. Для досягнення цієї мети було здійснено всебічний аналіз, який дозволив отримати комплексне розуміння проблеми, виявити основні загрози та ризики, а також сформувати ефективні рішення, здатні забезпечити надійний рівень захисту інформаційних ресурсів компанії.

У межах теоретичної частини роботи було детально розглянуто поняття кібербезпеки та ключові елементи її менеджменту. Аналіз наявної літератури та міжнародного досвіду засвідчив, що кібербезпека є багатовимірною та динамічною системою, яка охоплює не лише технічні, а й організаційні, правові та поведінкові аспекти. Важливим є дотримання міжнародних стандартів, зокрема ISO/IEC 27001 та GDPR, які встановлюють фундаментальні вимоги до захисту даних і процесів обробки інформації. Було встановлено, що ефективна система кіберзахисту потребує не лише впровадження технічних інструментів, а й стратегічного планування, побудови політики управління ризиками, а також активного залучення персоналу через формування культури інформаційної безпеки.

Проведений аналіз впливу кібербезпеки на ефективність операційної діяльності Heraeus Group продемонстрував прямий зв’язок між рівнем кіберзахисту та бізнес-результатами компанії. Зокрема, зменшення кількості кіберінцидентів у 2023 році з 124 до 45 супроводжувалося зниженням фінансових втрат із 20,5 до 11,8 млн євро, що свідчить про економічну вигоду інвестицій у безпеку. Значну увагу було приділено захисту критичної інфраструктури, насамперед SCADA-систем, які є життєво важливими для функціонування виробничих процесів. SWOT-аналіз виявив ключові сильні сторони компанії, такі як високий рівень автоматизації та ефективні системи моніторингу, водночас слабким місцем залишається застаріле обладнання, яке потребує модернізації.

Економічна оцінка заходів протидії кіберризикам показала їхню доцільність і фінансову ефективність. Найбільшу рентабельність інвестицій (ROI 210%) продемонстрували освітні програми для персоналу, які дали змогу знизити кількість інцидентів, спричинених людським фактором, на 25%. Модернізація SCADA-систем і впровадження принципу архітектури з нульовою довірою (zero-trust) забезпечили суттєву економію коштів — відповідно 1,8 млн євро та 1,4 млн євро. Також використання аутсорсингових послуг для моніторингу кіберінцидентів дозволило знизити витрати на відповідні функції на 30-40%, зберігаючи при цьому високу якість сервісу.

У результаті дослідження була сформована комплексна стратегія кібербезпеки, яка базується на поетапному підході до впровадження змін. Першочергова увага приділяється оновленню IoT-пристроїв, підвищенню обізнаності персоналу та впровадженню систем прогнозування загроз на основі штучного інтелекту й машинного навчання. До стратегії включено також впровадження георозподіленого резервного копіювання даних, що гарантує відновлення інформації навіть у разі масштабних атак. Одним із важливих елементів запропонованої стратегії є впровадження системи ключових показників ефективності (KPI), яка дозволяє в режимі реального часу оцінювати успішність впроваджених заходів та оперативно вносити необхідні корективи. Очікується, що реалізація цієї стратегії дозволить зменшити кількість успішних атак на 70-80%, скоротити середній час реагування до 10-15 хвилин і уникнути щорічних втрат на суму до 1,5 млн євро.

Практична значущість результатів дослідження полягає в можливості їх застосування на українських підприємствах, зокрема в галузях, де існує потреба в захисті критичних інфраструктурних об’єктів. Це стосується не лише великих виробничих компаній, а й малих та середніх підприємств, які мають обмежені бюджети, але прагнуть відповідати сучасним стандартам безпеки. Досвід Heraeus Group доводить, що навіть у складних умовах можливо досягти високого рівня захищеності за рахунок грамотної інтеграції технічних, організаційних і економічних рішень.

У підсумку дослідження підтвердило, що ефективна система управління кібербезпекою потребує цілісного підходу, який поєднує сучасні технології, системне управління ризиками, адаптивне планування й постійне вдосконалення внутрішніх процесів. Розроблені рекомендації можуть стати прикладом для впровадження на інших підприємствах, що прагнуть посилити свій захист у відповідь на зростаючі кіберзагрози. Перспективним напрямом для подальших досліджень є розгляд можливостей використання передових технологій, зокрема квантової криптографії, блокчейну та хмарних рішень нового покоління, що здатні суттєво підвищити надійність інформаційної інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Бакалінська О.О., Бакалинський О.О. Правове забезпечення кібербезпеки в Україні. Адміністративне право і процес, Київ, Гельветика, 2019. № 9. С. 100-106. DOI: https://doi.org/10.32849/2663-5313/2019.9.17 (дата звернення: 06.10.2024).
2. Бездітко О.Є. Управління фінансовими ризиками підприємства.
3. *Таврійський науковий вісник. Серія: Економіка*, Житомир: ПНУ, 2020. Вип. 3. С. 44-49. DOI: https://doi.org/10.32851/2708-0366/2020.3.6 (дата звернення: 18.11.2024).
4. Біленчук П.Д., Борисова Л.В., Неклонський І.М., Собина В.О.
5. Правові засади інформаційної безпеки України: монографія. Київ: Національний університет цивільного захисту України, 2018. С. 9-62. [Електроннийресурс]. - Режим доступу: http://repositsc.nuczu.edu.ua.handle/123456789/18077 (дата звернення: 10.10.2024).
6. Бурячок В.Л., Гнатюк С.О., Корченко О.Г. Кібернетична безпека держави: характерні знаки та проблемні аспекти. Київ: НАУ, *Український науковий журнал інформаційної безпеки*, том 19, вип. 1, 2013. С. 40-44 (дата звернення: 27.10.2024).
7. Василенко М., Горбаченко С., Слатвінська В., Чепурна О. Сценарне планування як інструмент безперервного бізнесу: web-технології (комплексний підхід). *Інформаційні технології та суспільство*, 2022. № 2 (4). С. 29-36 (дата звернення: 11.11.2024).
8. Василюк В. Об'єкти захисту інформації. Методи та засоби, 2006. С. 88-102.[Електронний ресурс]. - Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/fb3cf4e-273c-424e-aa24-1fddfc51943f/content (дата звернення: 15.10.2024).
9. Веселова, Л. Ю. Кібернетична безпека в умовах гібридної війни: адміністративно-правові засади. Запоріжжя: Гельветика, 2023. С. 284-321. [Електронний ресурс]. - Режим доступу: https://jurkniga.ua/kibernetichna-bezpeka-v-umovakh-gibridnoi-viyniadministrativnopravovizasadi/?srsltid

=Afm BOoqmB5OM08RHzw3etgbFv0lrRjMekuZXT30Dy29kJMbNh2ErbyRb (дата звернення: 30.10.2024).

10. Гапак О.М., Балога С.І. Захист інформації в комп'ютерних системах. Ужгород: ПП «АУТДОР-ШАРК», 2021. С. 14-29. [Електронний ресурс]. - Режим доступу: https://dspace.uzhnu.edu.ua/jspui/handle/lib/36506 (дата звернення: 08.12.2024).
11. Горбаченко С.А. Місце менеджменту кібербезпеки у сучасній управлінській науці та практиці. *Сталий розвиток економіки*, 2024. № 1(48). С. 144-149 (дата звернення: 06.11.2024). URL: https://economdevelopment.in.ua/index.php/journal/article/view/895 (дата звернення: 07.01.2025).
12. Горбаченко С.А., Бойко В.Д. Тестування на проникнення як ефективний інструмент менеджменту кібербезпеки. *Інформаційні технології та суспільство*, 2023. № 3. С. 23-29 (дата звернення: 21.10.2024).
13. Горбаченко С. А., Пейдж Н. Е. Цифрова трансформація управління персоналом у Industry 5.0: біоцентричний підхід. Харків, Державний біотехнологічний університет: *Журнал з менеджменту, економіки та технологій,* 2025. Вип. 1. С. 275-285. DOI: 10.69803/3083-6034-2025-1-275 (дата звернення: 18.04.2025).
14. Горбаченко С.А., Клєвцєвич Н.А. Роль кібербезпеки у впровадженні циркулярних економічних моделей: аналіз ризиків та можливостей. *Вісник Херсонського національного технічного університету,* 2024. № 1(88). С. 342-348 (дата звернення: 29.12.2024).
15. Горбаченко С.А., Клєвцєвич Н.А., Дикий О.В. Використання Big Data в процесі прийняття управлінських рішень. *Науковий погляд: економіка та управління*, 2024. № 4 (88). С. 127-135 (дата звернення: 25.10.2024).
16. Горбаченко С.А., Слатвінська В.М., Чепурна О.Є. Адаптація проєктного підходу до управління стартапами. *Трансформаційна економіка*, 2023. № 4 (04). С. 24-29 (дата звернення: 14.02.2025).
17. Горбаченко С.А., Соколов А.В., Клєвцєвич Н.А. Роль інформаційно-комунікаційних технологій в забезпеченні захисту інформації на рівні

територіальних громад. *Економічний вісник НТУУ «КПІ»*, 2024. № 29. С. 169-177 (дата звернення: 29.01.2025).

18. Горун О.Ю. Пріоритетні засади державної політики кібербезпеки: організаційно-правовий аспект. *Науковий фаховий журнал «Інформація і право»* №2 (37), 2021. С. 1-10. DOI: https://doi.org/10.37750/2616-6798.2021.2(37).238343 (дата звернення: 15.11.2024).
19. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки. Навчальний посібник. Київ: *НА СБУ*, 2020. С. 2-256. [Електронний ресурс]. Режим доступу: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_Metodol_ZahystuInfOsnKiberbezp_2020.pdf (дата звернення: 09.11.2024).
20. Документ 2163-VIII, чинний, поточна редакція. Редакція від 24.10.2020, підстава 912-IX. Про основні засади забезпечення кібербезпеки України. С. 1-25. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 15.01.2025).
21. Долгальова О.В., Ремесник Т.С. Застосування зарубіжних методів мотивації праці на українських підприємствах. *Галицький економічний вісник.* Том 70. Вип. № 3, 2021, С. 140-146. [Електронний ресурс]. - Режим доступу: https://galicianvisnyk.tntu.edu.ua/pdf/70/983.pdf (дата звернення: 02.12.2024).
22. Заріцький О.В., Корченко А.О. Програмне забезпечення для формування еталону параметрів систем виявлення кібератак. *Український журнал досліджень інформаційної безпеки* 20(3), 2018. С. 133-148 (дата звернення: 10.12.2024).
23. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: АртЕк, 2018. С. 207-278. [Електронний ресурс]. - Режим доступу: https://ru.scribd.com/document/775575162/Монографія-О-золотар-Інфор маційна-Безпека (дата звернення: 05.10.2024).
24. Корченко, О.Г., Гнатюк, С.О., Казмірчук С.В., Панченко В.М., Мельник С.В. Аудит та управління інцидентами інформаційної безпеки. Навчальний посібник. Київ: Національна академія Служби Безпеки

України, 2014. С. 7-143. [Електронний ресурс]. - Режим доступу: http://er.nau.edu.ua/handle/NAU/38027 (дата звернення: 12.10.2024).

25. Куцик П.О., Туліка Н.М., Процикевич А.І. Стан та перспективи розвитку ІТ-індустрії України. Львів: *Економіка та суспільство*, 2024. Вип. 67. С. 1-7. DOI: https://doi.org/10.32782/2524-0072/2024-67-108 (дата звернення: 04.01.2025).
26. Омельченко А. В. Організаційно-правові засади забезпечення кібербезпеки України. *Київський часопис права*, 2022. Вип. 3. 140-145. DOI: https://doi.org/10.32782/klj/2021.3.22 (дата звернення: 27.01.2025).
27. Пейдж Н. Е. Державно-правова база легітимізації боротьби з кіберзлочинами. Національний університет «Одеська юридична академія»: *Матеріали Всеукраїської науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики»,* 25 листопада 2022 року, м. Одеса, 2022. С. 191-193.
28. Резворович К.Р., Юнін О.С., Круглова О.О. та інші. Фінансовоекономічна безпека: теоретико-правові аспекти. Видавець Біла К.О., 2019. С. 38-53 (дата звернення: 24.11.2024).
29. Степко О.М. Аналіз головних складових інформаційної безпеки держави. Київ: НАУ, 2013. Том 1, Вип. № 3, С. 90-98 (дата звернення: 11.02.2025).
30. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері,* 2018. С. 75-82. DOI: https://doi.org/10.31866/2617-796x.1.2018.147257 (дата звернення: 09.01.2025).
31. Atle R., Bjornar S., Ketil S. Cyber-Risk Management. New York City: Springer International Publishing, 2015. P. 5-101 (дата звернення: 30.11.2024).
32. Avelar V., Azevedo D., Emerson A. F. Pue: a comprehensive Examination of the metric. The green grid, 2012. P. 9-83 (дата звернення: 01.01.2025).
33. Bilge L., Dumitras T. Before we knew it: an empirical study of zero-day attacks in the real world. Нью-Йорк: Association for Computing Machinery, 2012. P. 833-844 (дата звернення: 17.03.2025).

34. Brian Z. The practical application of ISO 22301. *Journal of Business Continuity & Emergency Planning*, 2014. P. 83-90 (дата звернення: 26.10.2024).
35. Bruno C. Implementation of new legislative measures on industrial risks prevention and control in urban areas. *Journal of Hazardous Materials,* 2006. P. 293-299 (дата звернення: 30.12.2024).
36. Carol A. The Present and Future of Financial Risk Management. *Journal of Financial Econometrics,* 2005. Vol. 3, Issue 1. P. 3-25 (дата звернення: 05.12.2024).
37. Cappello M., Καππέλλο M. A comprehensive analysis of EDR (Endpoint Detection & Response), EPP (Endpoint Protection Platform), and antivirus security technologies. ELiDOC: *Master Thesis*, 2024. P. 9-24 (дата звернення: 08.10.2024).
38. Clemens S.K., Benjamin F., Taylor J., Kyle D.M. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technol Health Care*, 2017. Vol. 25(1). P. 1-10 (дата звернення: 21.12.2024). DOI: https://doi.org/10.3233/THC-161263, дата звернення: 03.02.2025.
39. Craft. Heraeus Financials [Електронний ресурс]. - Режим доступу: https://craft.co/heraeus/financials (дата звернення: 25.10.2024).
40. Davis M. R. The data encryption standard in perspective. Published in IEEE Communications Society, 1978. P. 5-9 (дата звернення: 14.01.2025.)
41. Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Springer Publisher, 2011. P. 497-501. [Електронний ресурс]. - Режим доступу: https://link.springer.com/chapter/10.1007/978-3-642-22540-6_48 (дата звернення: 18.10.2024).
42. Dodis Y., Haralambiev K., Lopez-Alt A., Wichs D. Cryptography Against Continuous Memory Attacks. U.S., New York City: IEEE Publisher, 2010. P. 1-10. [Електронний ресурс]. - Режим доступу: https://ieee-focs.org/FOCS-2010-Papers/Cryptography-Against-Continuous-Memory-Attacks.pdf (дата звернення: 28.12.2024).

43. Evans A. Enterprise Cybersecurity in Digital Business: Building a Cyber Resilient Organization. Springer Publisher, 2022. 562 p. (дата звернення: 08.03.2025).
44. European Union Agency for Cybersecurity. *ENISA Threat Landscape*, 2024, P. 2-32 (дата звернення: 27.10.2024).
45. Geeta Y., Kolin P. Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection*, 2021. P. 50-71 (дата звернення: 30.12.2024).
46. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018. P. 3-99. [Електронний ресурс]. - Режим доступу: https://gdpr-info.eu/ (дата звернення: 22.01.2025).
47. Gloham A.A., Maryam M., Aghdas N. Organizational Structure. *Procedia - Social and Behavioral Sciences*, 2016. Vol. 230. P. 455-462. [Електронний ресурс]. - Режим доступу: https://www.studocu.com/row/document/ethiopian-civil-service-university/businessmanagement/organizationalstructure/84053140 (дата звернення: 01.10.2024).
48. Greis J., Sorel M., Fuchs-Souchon J., Banerjee S. The cybersecurity provider's next opportunity: Making AI safer, 2024. [Електронний ресурс]. - Режим доступу: https://ramaonhealthcare.com/the-cybersecurity-providers- next-oppor tunity-making-ai-safer/ (дата звернення: 23.10.2024).
49. Heinl M., Pursche M., Puch N., Peters S. N. & Giehl A. ISA/IEC 62443 Accenture, 2024. State of Cybersecurity Resilience: *Industrial Manufacturing Report.* Springer Publisher, 2024. P. 196-210 (дата звернення: 09.03.2025).
50. Heraeus Group. Investor Relations. Heraeus Group Official Website. [Електронний ресурс]. - Режим доступу: https://www.heraeus-group.com/en/about-heraeus/investor-relations/ (дата звернення: 17.10.2024).
51. Heraeus Precious Metals Factbook 2023 [Електронний ресурс]. - Режим доступу: https://www.heraeus-precious-metals.com/dam/jcr:33d11ad4-4b6b-4b7c-8fa0-e6efd33bf85c/heraeus-precious-metals-factbook-2023-en.pdf (дата звернення: 28.10.2024).

52. Information Security Management Systems - Requirements. International Organization for Standardization. P. 19. [Електронний ресурс]. - Режим доступу: https://www.iso.org/standard/27001, ISO/IEC 27001:2022 (дата звернення: 18.01.2025).
53. Jacobs F. R., Whybark D. C. Why Erp? a Primer on Sap Implementation. McGraw-Hill Higher Education, 2000. P. 144 (дата звернення: 11.12.2024).
54. Jacobson R. The Validity of ROI as a Measure of Business Performance. American Economic Association, 1987. P. 470-478 (дата звернення: 31.10.2024).
55. Jiajun L., Zhaoying J., Fen W. Construction of enterprise comprehensive management system based on information reconstruction and IoT. *International Journal of System Assurance Engineering and Management*, 2024, № 7, P. 2914-2930. [Електроннийресурс].- Режим доступу: https://ouci.dntb.gov.ua/ en/works/lDLAP0Ml/ (дата звернення: 16.12.2024).
56. Kim P. The Hacker Playbook: Practical Guide to Penetration Testing (1th ed.). CreateSpace Independent Publishing, 2014 P. 5-101 (дата звернення: 19.01.2025).
57. Krak N.C, R. Boellaard, Hoekstra O.S., Twisk J.W.R, Hoekstra C.J., Lammertsma A.A. Effects of ROI definition and reconstruction method on quantitative outcome and applicability in a response monitoring trial. *European Journal of Nuclear Medicine and Molecular Imaging,* 2004. Vol. 32 P. 294-301 (дата звернення: 06.03.2025).
58. Liu A.X. Diverse Firewall Design. IEEE Publisher, 2008. P. 1237-1251 (дата звернення: 23.11.2024).
59. McClure S., Scambray J., Kurtz G. Hacking Exposed 7: Network Security Secrets and Solutions. McGraw Hill, 2012. P. 235-258 (дата звернення: 04.10.2024).
60. Mesquida A.L., Mas A., Esperança A., Calvo-Manzano J.A. IT Service Management Process Improvement based on ISO/IEC 15504: *A systematic review*. Elsevier, 2011. P. 239-247 (дата звернення: 25.12.2024).

61. Mizrak F. Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Beykoz University, 2023. Vol. 10, Issue 3. P. 1-12. DOI**:** https://doi.org/10.17261/Pressacademia.2023.1807 (дата звернення: 12.01.2025).
62. Nagendrababu N. C, Samyama Gunjal G.H, Himabindhu N. T. Advance persistent threat prediction using knowledge graph. *International Journal of Science and Technology Research*, 2024. P. 1-12 (дата звернення: 19.02.2025).
63. Nankya M., Chataut R., Akl R. Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. MDPI, 2023. P. 1-10 (дата звернення: 14.12.2024).
64. NIST.Framework for Improving Critical Infrastructure Cybersecurity Version 2.0. *A Practical Guide with Examples*, 2024. P. 1-32. [Електронний ресурс]. - Режим доступу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST. CSWP.29.pdf (дата звернення: 15.01.2025).
65. Olaniyan D.A., Ojo L.B. Staff Training and Development: A vital tool for organisational effectiveness. *Euro Journals Publishing*, 2008. Vol. 24. No.3. P.326-331. [Електронний ресурс]. - Режим доступу: https://tarjomefa. com/wp-content/uploads/2017/07/7006-English-TarjomeFa.pdf (дата звернення: 26.11.2024).
66. Ozcan S., C. Okan S., Suloglu M. Human Resources Mining for Examination of R&D Progress and Requirements. Leeds University: IEEE Publisher, 2020. P. 1372-1387 (дата звернення: 27.10.2024).
67. Page N. A. Music information as a factor of progress in educational institutions of England. *Міжнародна науково-творча конференція «Захід-Схід: культура та мистецтво. Пам'яті видатних митців України присвячується,* 25-26 вересня 2022 року, м. Одеса. Збірник наукових праць. С.182-185.
68. Page N. A. Technologies through the prism of human values and organizational culture. *Міжнародний Фестиваль-Конференція «Захід* -

Схід: культура і сучасність - на славу знаних митців Одеси», 28-29 вересня 2024 року, м. Одеса. Збірник наукових праць. С.201-204.

69. Page N. A. The impact of hybrid threats on the cyber security of critical infrastructure in the context of modern global challenges. *Національний університет «Одеська юридична академія»: Матеріали Всеукраїської науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики»*, 22 листопада 2024 року, м. Одеса, 2024. С. 161-163.
70. Page N. A. Corporate Philosophy and Culture: The Role and Functions of a Manager. *Міжнародна науково-творча конференція трансформація музичної культури і освіти: пам'яті витоків і звершень першого музичного ВИШУ України,* 11-13 травня 2024 року, м. Одеса. 2024. С. 280-283.
71. Radouan A.M. Internet of Things (IoT). *Journal of Data Analysis and Information Processing*. 2021. Vol. 9, No. 2. P. 1-25 (дата звернення: 14.10.2024).
72. Saqib Saee, Salha A.A, Norah A.A, Ebtisam Alshehri. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, 2023. P. 1-20. [Електронний ресурс]. - Режим доступу: https://www.mdpi.com/1424-8220/23/15/6666 (дата звернення: 21.03.2025).
73. Samiksha S. Investigating an association between DDoS and phishing attacks. University of Twente, 2021. P. 2-26 (дата звернення: 02.01.2025).