Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

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

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____

_____Технології забезпечення фінансової безпеки підприємства_____
_____в умовах цифрової економіки_____
(тема)

Виконав:
студент _2_ курсу, групи _УФЕБм-21-1____
_____Давіденко А. І._____
(прізвище, ініціали)

Спеціальність 073 Менеджмент_____
_____ (код і повна назва спеціальності)
Тип програми ___освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма _Управління фінансово-економічною безпекою_____
(повна назва освітньої програми)

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

Допускається до захисту

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

2022 р.

Харківський національний університет радіоелектроніки

Факультет__інформаційно-аналітичних технологій та менеджменту_____
(повна назва)

Кафедра_економічної кібернетики та управління економічною безпекою___
(повна назва)

Рівень вищої освіти __другий (магістерський)_____

Спеціальність _____073 Менеджмент_____
(код і повна назва)

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

Освітня програма _____Управління фінансово- економічною безпекою___
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові_____Давіденко Анастасії Ігорівні_____
(прізвище, ім'я, по батькові)

1. Тема роботи _Технології забезпечення фінансової безпеки підприємства в умовах цифрової економіки_____
_____
затверджена наказом університету від _07_ _листопада_2022 р. № _1452 Ст_____
2. Термін подання студентом роботи до екзаменаційної комісії _19_ _грудня_ 2022 р.
3. Вихідні дані до роботи _Фінансова звітність підприємства, періодичні видання, наукова література, інформаційні ресурси мережі Інтернет_____
_____
_____
_____
_____
_____
_____
4. Перелік питань, що потрібно опрацювати в роботі Вступ. 1. Теоретичні основи забезпечення фінансової безпеки в умовах цифрової економіки. 2. Аналіз діяльності та забезпечення фінансової безпеки компанії «Cisco». 3. Удосконалення технологій забезпечення фінансової безпеки компаній в умовах цифрової економіки. Висновки. Перелік джерел посилань. Додатки._____
_____
_____
_____
_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 1-3. Об'єкт, предмет, мета і завдання дослідження, наукові результати. 4. Завдання конкурентної розвідки. 5. Структура методів аналізу інформації. 6. Типи ключових факторів успіху забезпечення економічної безпеки. 7-11. Аналіз діяльності. 12. Модель системи економічної безпеки. 13. Матрична система забезпечення економічної безпеки. 14. Структура і функції підрозділу конкурентної розвідки та інформаційного забезпечення безпеки.

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

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

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Виконання першого розділу роботи	01.11. 2022-08.11. 2022	виконано
2	Виконання другого розділу роботи	09.11. 2022-19.11. 2022	виконано
3	Виконання третього розділу роботи	20.11. 2022-27.11. 2022	виконано
4	Оформлення роботи	28.11. 2022-03.12. 2022	виконано
5	Перевірка роботи на плагіат	04.12. 2022-09.12. 2022	виконано
6	Підготовка доповіді та ілюстративного матеріалу	10.12. 2022-15.12. 2022	виконано
7	Рецензування роботи	16.12.2022-18.12. 2022	виконано
8	Подання роботи до екзаменаційної комісії	19.12.2022	виконано

Дата видачі завдання _01 листопада___2022 р.

Студент _____
(підпис)

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

РЕФЕРАТ

Кваліфікаційна робота: 68 с., 6 табл., 18 рис., 42 джерела, 2 додатки.

ФІНАНСОВО-ЕКОНОМІЧНА БЕЗПЕКА, ЦИФРОВА ЕКОНОМІКА, ОЦІНКА, РІВЕНЬ, ФІНАНСОВИЙ МЕХАНІЗМ.

Об’єкт дослідження – компанія «Cisco».

Мета дослідження – теоретичне обґрунтування та розробка системи забезпечення безпеки з урахуванням новітніх технологій цифрової економіки.

Розглянуто методичні аспекти оцінки рівня фінансово-економічної безпеки підприємства. Розкрито теоретичні засади управління фінансово-економічною безпекою підприємства. Проаналізовано сучасні технології цифрової економіки, та її вплив на рівень фінансово-економічної безпеки компанії. Проаналізовано діяльність та напрями організації безпеки компанії «Cisco». Розроблено систему забезпечення безпеки компанії з урахуванням новітніх технологій цифрової економіки. Розроблена технологічна складова системи забезпечення безпеки компанії. Розроблену систему та технологічну розробку запропоновано для компанії «Cisco».

ABSTRACT

Master’s thesis: 68 p., 6 tables, 18 fig., 42 sources, 2 exhibit.

THE FINANCIAL-ECONOMIC SECURITY, ESTIMATION, LEVEL, INTEGRAL FACTOR.

The object of the research is the company «Cisco».

The purpose of the study is the theoretical substantiation and development of a security system taking into account the latest technologies of the digital economy.

Methodological aspects of assessing the level of financial and economic security of the enterprise are considered. The theoretical principles of managing the financial and economic security of the enterprise are revealed. Modern technologies of the digital economy and their impact on the level of financial and economic security of the company are analyzed. The activities and directions of the security organization of the company «Cisco» have been analyzed. The company's security system was developed taking into account the latest technologies of the digital economy. The technological component of the company's security system has been developed. The developed system and technological development are proposed for the company «Cisco».

ЗМІСТ

ВСТУП

В умовах економічної та політичної нестабільності функціонування підприємств сильно залежить від обґрунтованих та виважених управлінських рішень та ефективних систем організації діяльності. Через відсутність чіткого напряму розвитку та якісну стратегію управління розвитком вітчизняним підприємствам складно вирішувати ці завдання, що призводить до зниження фінансової стійкості, потенціалу та конкурентоспроможності підприємств.

На сучасному етапі розвитку української економіки діловий стан вітчизняних підприємств явно тяжкий. Ефективність діяльності суб'єкта залежить від його фінансового стану, у зв'язку з чим необхідно враховувати питання забезпечення фінансової безпеки суб'єкта.

В даний час відбувається четверта промислова революція, і нові технології з'являються і в галузі корпоративної безпеки. Пропонується проаналізувати ринок охоронних послуг та досвід компаній, що їх реалізують.

Об’єктом дослідження є компанія «Cisco».

Метою дослідження є – теоретичне обґрунтування та розробка системи забезпечення безпеки з урахуванням новітніх технологій цифрової економіки.

Завдання роботи:

– проаналізувати теоретичні основи безпеки підприємства;

– розглянути актуальні новітні технології забезпечення безпеки;

– дослідити специфіку діяльності великої технологічної компанії «Cisco»;

– обґрунтувати рішення з формування системи безпеки підприємства;

– запропонувати алгоритм та технологічну розробку для забезпечення безпеки підприємства.

Інформаційними джерелами для проведення дослідження стали наукові праці провідних фахівців в області аналізу, забезпечення безпеки підприємства, оцінки ступеня ризику.

Практична цінність роботи полягає в тому, що запропонована система дозволяє отримати та використовувати «базу знань» з теми фінансової безпеки з урахуванням новітніх технологій.

Особливістю запропонованої схеми покроковий алгоритм дій для захисту підприємства.

Апробація результатів дослідження. Основні теоретичні положення і практичні результати проведених досліджень, висновки і рекомендації, які викладені в роботі, доповідались на I Міжнародній науково-практичній конференції «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта» (Харків. 3 листоп. 2020) та I Всеукраїнській науково-практичній конференції «Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці» *(*Київ, 7 грудня 2020 р.).

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

1.1 Фінансовий механізм як складова безпеки підприємства

Фінансовий механізм підприємства це невід'ємна частина господарського механізму підприємства; сукупність форм та методів забезпечення підприємства необхідними засобами для досягнення нормального рівня стійкості та ліквідності, забезпечення ефективної роботи господарства та максимізації прибутку.

Фінансовий механізм підприємства – це різновид системи управління фінансами, що є сукупністю форм і методів, що дозволяють підприємствам здійснювати такі види діяльності: забезпечувати себе необхідними засобами, досягти нормального рівня стабільності та плинності, забезпечення рентабельності операцій та максимального прибутку. Фінансовий механізм складається з двох підсистем:

- підсистема управління. До нього входять фінансові служби підприємства та його відділи, тому основним органом управління фінансовим механізмом є фінансові служби та його відділи, а також фінансові менеджери;
- до керованих підсистем належать: фінансові відносини; джерело фінансових ресурсів; фінансові ресурси підприємства; фінансовий оборот підприємства.

Об'єктом управління фінансового механізму є грошовий оборот підприємства, що є безперервним рухом грошових надходжень і платежів за розрахунковими та іншими рахунками підприємства [1].

Структура фінансового механізму підприємства включає п'ять взаємопов'язаних елементів: фінансові кошти, фінансовий важіль, правове, нормативно-правове та інформаційне забезпечення.

Фінансові методи – способи впливу фінансових відносин на економічні процеси, освіту та використання коштів.

Фінансовий важіль – це інструмент, який використовується у фінансових методах. До них відносяться: прибуток, виторг, та ін.

Забезпечення функціонування фінансового механізму компанії містить законодавчі акти, розпорядження, укази, циркулярні послання та ін. правові папери органів керування.

Нормативне забезпечення функціонування фінансового механізму підприємства враховує застосування загальновизнаних мірок та нормативів використовуваних грошей, демпферних загальновизнаних мірок, тарифних та податкових ставок.

Інформативне функціонування фінансового механізму компанії полягає з різного сімейства і типу фінансової, комерційної, економічної та ін. інформації. До даної інформації зараховуються: дані щодо економічної стабільності та платоспроможності партнерів та конкурентів, щодо вартості, курси грошових одиниць, дивіденди, відсотки в товарному, фондовому та грошовому ринках і т.п. [2].

Безпека підприємства – це комплексна програма, яка забезпечує загальну безпеку бізнесу за допомогою доступних безпекових технологій.

Управління безпекою підприємства – це стратегія, яку компанії використовують для зменшення ризику несанкціонованого доступу до систем та даних інформаційних технологій [3].

Діяльність з управління безпекою підприємства передбачає розробку, інституціоналізацію, оцінку та вдосконалення політики управління ризиками підприємства (ERM) та безпеки. Управління безпекою підприємства передбачає визначення того, як різні бізнес-підрозділи, співробітники, менеджери та персонал повинні працювати разом, щоб захистити цифрові активи організації, забезпечити захист від втрати даних та захистити громадську репутацію організації.

Безпека підприємства має наступні складові (рис 1.1.)

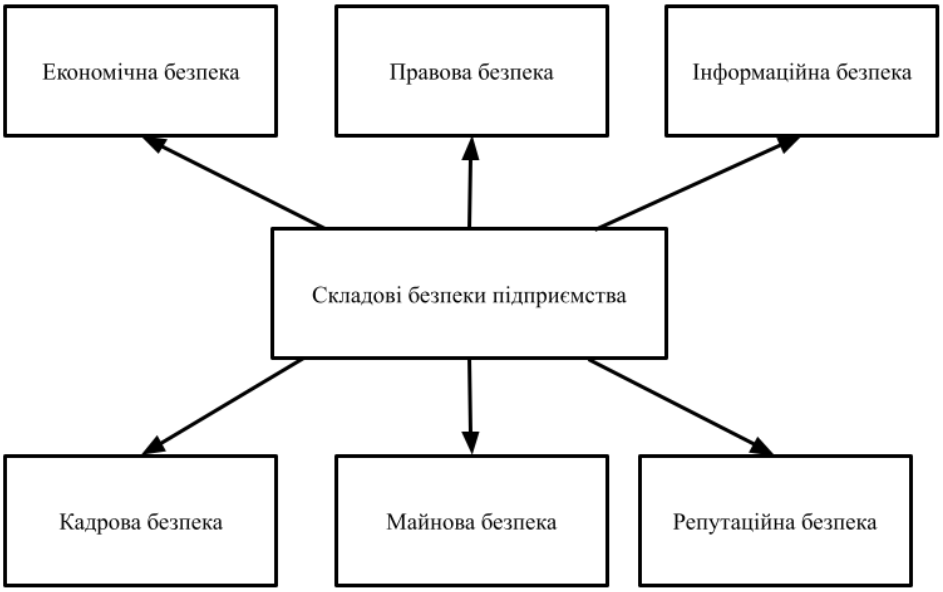


Рисунок 1.1 – Складові безпеки підприємства

Ці компоненти наражаються на такі ризики:

– підприємницький ризик. Ризики, пов'язані з репутацією, запровадження нових розробок, які можуть виявитися невдалими;

– інформаційний ризик. Витік інформації, загроза її цілісності, заміна, утруднення доступу до даних, сервісів та додатків;

– кадровий ризик. Відтік кадрів, конкуренція за залучення цінних працівників, завдання охорони праці, зниження виробничого травматизму та захворюваності за важких та шкідливих умов праці;

– небезпека інфраструктури. Відмова чи зламання обладнання, аварія;

– валютний ризик. Крадіжка, пошкодження, втрати, штрафи, судові збитки [4].

Професійна робота, побудована на єдиній стратегії, системі та використанні сучасних програмних засобів, допоможе захистити компанії від більшості ризиків.

Для розв'язання проблем, пов'язаних з цими ризиками, необхідно побудувати систему безпеки підприємства

Механізм боротьби з загрозами, складається з етапів:

– виявлення ризиків. Персонал організації повинен розробити механізм виявлення загроз для запобігання хибним спрацьовуванням. Так, для IT-фахівців розв'язання проблеми – наявність системи моніторингу IT-інфраструктури, для оповіщення про вторгнення, для внутрішніх перевірок – відхилень результатів фінансово-господарської діяльності від звичайних значень сезонності чи інших коливань;

– аналіз. Співробітники повинні передбачати ймовірність загроз, оцінювати їх масштаби, знаходити джерела та заходи протидії як самостійно, так і за участю відповідних підрозділів;

– протистояння. Для кожного виду загроз має бути своя політика чи директива, що дозволяє швидко діяти самостійно, вибираючи правильну з дерева рішень;

– регулювання. Усі етапи роботи з погрозами Внутрішню безпеку підприємства повинні бути регламентовані в чітких інструкціях, прийнятих на рівні керівництва компанії [5].

Тому виникає необхідність реалізувати стратегію безпеки підприємства, під якою розуміється сукупність найбільш значущих рішень, вкладених у забезпечення прийнятного рівня безпеки функціонування підприємства.

Розрізняють такі типи стратегій безпеки:

– зосередження на усуненні наявних або запобігання потенційним загрозам;

– призначена для запобігання впливу наявних або потенційних загроз безпеці;

– призначена для відновлення (компенсації) завданих збитків.

Засоби та методи забезпечення безпеки. Серед наявних заходів безпеки можна назвати такі:

– технічні засоби. До них належать системи безпеки та протипожежного захисту, відео-радіообладнання, засоби виявлення вибухових пристроїв, бронежилети, загородження та багато іншого;

– організаційні засоби. Створення спеціальної організаційної структури задля забезпечення безпеки підприємства;

– засоби інформації. Насамперед це друкована та відеопродукція щодо захисту конфіденційної інформації. Крім того, критично важлива інформація, що використовується для прийняття рішень щодо безпеки, зберігається на комп'ютерах;

– фінансові ресурси. без достатніх фінансових ресурсів робота системи безпеки неможлива, питання лише у тому, як їх використовувати цілеспрямовано та з високою віддачою;

– правові засоби. Мається на увазі використання не лише законів та підзаконних актів, що видаються вищими органами, а й розробка локальних правових актів щодо безпеки;

– кадрові ресурси. По-перше, це стосується достатності кадрів для розв'язання питань безпеки. У цьому вирішують завдання підвищення кваліфікації у сфері діяльності;

– інтелектуальні засоби. Залучення висококваліфікованих фахівців, науковців (іноді доцільно залучати їх із боку) дає змогу впроваджувати нові системи безпеки [6].

Слід зазначити, що застосування кожного з перерахованих вище засобів окремо не дає належного ефекту, як у комплексі. Застосування перерахованих вище засобів зазвичай розбивають на кілька етапів:

– I етап. Розподіл фінансових ресурсів;

– II етап. Навчання кадрів та організаційних ресурсів;

– III етап. Розвиток системи правових засобів;

– IV етап. Залучення технічних, інформаційних та інтелектуальних засобів.

При переведенні зі статичного стану динамічний вищевказані кошти стають методами, тобто методами, прийомами дії. Отже, можна говорити про технічні, організаційні, інформаційні, фінансові, правові, кадрові та інтелектуальні методи. Функції даних методів:

– технічні – спостереження, контроль, ідентифікація тощо;

– організаційні – створення охоронних зон, режиму, розслідувань, постів, патрулів тощо;

– інформативні – розробка характеристик на співробітників, аналітичні матеріали конфіденційного характеру тощо;

– матеріальне заохочення – матеріальне для співробітників, які мають досягнення у забезпеченні безпеки, матеріальне заохочення інформаторів тощо;

– юридичні – захист законних прав та інтересів, допомога правоохоронним органам та ін.;

– персонал – підбір, розставляння та навчання персоналу для забезпечення безпеки підприємства, його навчання тощо;

– інтелектуальні – патенти, ноу-хау тощо [7].

Концепція безпеки. Концепція визначається як система точок зору, ідей, цілей, пронизана єдиною визначальною ідеєю, керівною думкою, що містить постановку та розв'язання зазначених проблем.

Концепція безпеки підприємства – це офіційно затверджений документ, що відображає систему поглядів, вимог та умов на організацію заходів щодо забезпечення безпеки персоналу та майна на підприємствах [8]. Зразкова концептуальна структура може мати наступний вигляд.

Опис проблемної ситуації у сфері корпоративної безпеки:

– список потенційних та актуальних загроз безпеці, їх рейтинги та рейтинги;

– джерела та фактори загроз;

– негативні наслідки загроз компанії.

Механізм безпеки:

– визначення охоплення та цілей соціального забезпечення;
– розробка політику та стратегію безпеки;
– принципи безпеки;
– цілі безпеки;
– функції безпеки;
– корпоративні стандарти та показники безпеки;
– створення організаційної структури управління системою безпеки компанії.

Заходи щодо реалізації заходів безпеки:

– формування підсистем загальної системи безпеки компанії;
– Визначення об'єктів безпеки підприємства та їх ролей;
– розрахунок коштів та визначення способів забезпечення;

Управління та оцінка процесу реалізації концепції.

Зазначимо, що найповніше уявлення про систему безпеки підприємства виходить після розгляду офіційно прийнятого документа про концепції безпеки підприємства, комплексної програми безпеки підприємства та плану відділу підприємства щодо реалізації цієї програми. потрібно. Доказова система безпеки підприємства є організаційною основою створення структурного підрозділу служби безпеки.

1.2 Розвиток цифрової економіки як нові можливості та нові виклики для фінансового механізму підприємства

Цифровізація викликала нову хвилю інновацій що матиме глибокі наслідки для людства, змінюючи відносини між громадянами, Уряди та підприємства, і це змінить структуру суспільства та економіки.

Зростання, продуктивність і людський розвиток дедалі більше визначатимуться рівнем інтеграції в цифрову економіку. Дійсно, цифровізація та передові технології не тільки створюють нові можливості для ведення бізнесу, вони також створюють низку виклики та ризики [9].

Цифрові технології та платформи можуть зменшити трансакційні витрати для бізнесу та полегшити доступ до нових клієнтів, як на внутрішньому, так і на зовнішньому ринках. Цифровізація може підвищити продуктивність підприємств і пропонувати нові можливості для підприємництва, інновацій та створення робочих місць. Це може допомогти бізнесу, зокрема мікро-, малим і середнім підприємствам подолати перешкоди для розширення та дозволити їм брати участь у рівноправній співпраці в інновації та використовувати альтернативні механізми фінансування, такі як краудфандинг (колективне співробітництво людей, які добровільно поєднують гроші та інші ресурси, зазвичай через Інтернет, для підтримки зусиль інших організацій).

Електронна комерція може полегшити розширення таких підприємств шляхом надання можливостей фінансування та засобів для побудови, які можна перевірити онлайн-записи транзакцій, які можуть допомогти залучити нових клієнтів і ділових партнерів [10].

Зараз світ перебуває на етапі четвертої промислової революції.

Четверта промислова революція (Industry 4.0) – це концепція, яка передбачає розвиток і злиття автоматизованого виробництва, обміну даними та виробничих технологій в єдину систему з незначним втручанням людини у виробничий процес або без нього взагалі.

Industry 4.0 дозволить збирати та аналізувати дані з різних машин, забезпечуючи швидші, ефективніші та гнучкіші процеси для виробництва товарів вищої якості за нижчими цінами. Ця революція також породила абсолютно нові бізнес-моделі, які сприятимуть новим способам взаємодії в ланцюжку створення вартості [11].

Складові Industry 4.0.

У роботі «Design Principles for Industrie 4.0 Scenarios» автори визначають наступні ключові компоненти:

– кіберфізична система (КФС) – це інтегрована комп'ютерна та мережева технологія, яка дозволяє спостерігати, контролювати та отримувати зворотний зв'язок щодо фізичних виробничих процесів;

– інтернет речей – це поєднання різних компонентів (датчиків, смартфонів тощо) через Інтернет, що дозволяє їм взаємодіяти один з одним для досягнення спільної мети;

– інтернет послуг – надання послуг постачальниками через інтернет;

– розумний завод – це фабрики, де обладнання автоматизоване, кероване комп'ютерами та може використовувати датчики для отримання зворотного зв'язку про стан об'єктів у фізичному просторі.

Сучасний етап промислової революції пов'язаний з розвитком комунікаційних технологій інтернету, які суттєво змінили технологію бізнес-процесів. У результаті цифрова економіка стала основою для четвертої промислової революції та третьої хвилі глобалізації [12].

Під цифровою економікою розуміється використання цифрових інструментів та передових технологій, таких як мобільні додатки, соціальні мережі та електронна комерція у повсякденному бізнесі.

Цифрова економіка фокусується на двох ключових принципах: інформаційних та мережевих технологіях. Електронні дані є важливим стратегічним ресурсом для оцифрування. Сучасні IT-інструменти, включаючи бізнес-моделі, розробляються та розробляються для використання інформації. Суть та значення цифрової економіки полягає у прискоренні механізмів обміну великими обсягами електронної інформації між учасниками та спрощенні повсякденних процесів. Нові напрямки розвитку не лише створюють нові можливості, але й стикаються з новими проблемами, тому

постає питання «Чи потрібно використовувати такі технології?» Розглянемо плюси і мінуси використання:

Плюси:

– орієнтованість на сучасний ринок;

– розвинутий захист даних;

– розвинута фінансова безпека.

Мінуси:

– неможливість перейти на новітні технології, це залежить від формату бізнесу;

– коштовність впровадження технологій в бізнес [13].

Для того, щоб побудувати стійку цифрову економіку, кожна організація повинна розглянути питання щодо переведення свого бізнесу на доступні цифрові платформи, які пропонують оптимізацію, інновації та взаємодію з клієнтами.

Стійка цифрова економіка виникає не лише завдяки зв'язності цифрових платформ та технологій, а й завдяки швидкості організаційних інновацій та адаптації.

Тому насамперед цифрова адаптація в економічному масштабі є фактором сталої цифрової економіки. Зрештою, цифрова модернізація повинна бути адаптована до індивідуальних бізнес-моделей, що існують у кожній країні, щоб забезпечити стійку цифрову економіку та інновації [14].

З розвитком цифрової економіки компаніям стає дедалі важче зберігати лідерство над ринком, тому важливо вимірювати взаємозв'язок між цифровою економікою, стійкістю, соціальними реформами та механізмами управління. Єдиний спосіб, за допомогою якого компанії можуть залишатися конкурентоспроможними, — йти в ногу із цифровою трансформацією економіки [15].

Об’єднуючи наведені вище факти, можна зробити висновок, що цифрова економіка продовжує розвиватися з високою швидкістю, керуючись

можливістю збирати, використовувати та аналізувати великі обсяги інформації (цифрових даних).

1.3 Сучасні технології цифрової економіки

1.3.1 Аналіз сучасних технологій для забезпечення фінансової безпеки в умовах цифрової економіки

Розвиток цифрової економіки радикально змінив пропозицію товарів і послуг через скорочення операційних і посередницьких витрат і використання інформації зі згенерованих даних на цифрових платформах. Так цифрові механізми полегшують генерацію та збір даних, які, при обробці та аналізі за допомогою розумних інструментів можна використовувати для покращення прийняття рішень і оптимізації постачання.

Це призводить до більш раціоналізованих операційних процесів, сегментації ринку та персоналізації продукту. Дані та цифрові знання стають стратегічним фактором виробництва. Це тягне за собою необхідність регулятивних змін у різноманітних сферах, починаючи від телекомунікацій і закінчуючи торгівлею, впроваджуючи політики щодо конкуренції, захисту даних і кібербезпеки [16].

Цифрові технології відіграють все більшу роль у нашому суспільстві. Оскільки здатність підключатися та швидко й ефективно взаємодіяти стає важливою, цифрові навички стають все більш актуальними для бізнесу та громадян.

Елементи цифрової економіки наведені на рис. 1.2.

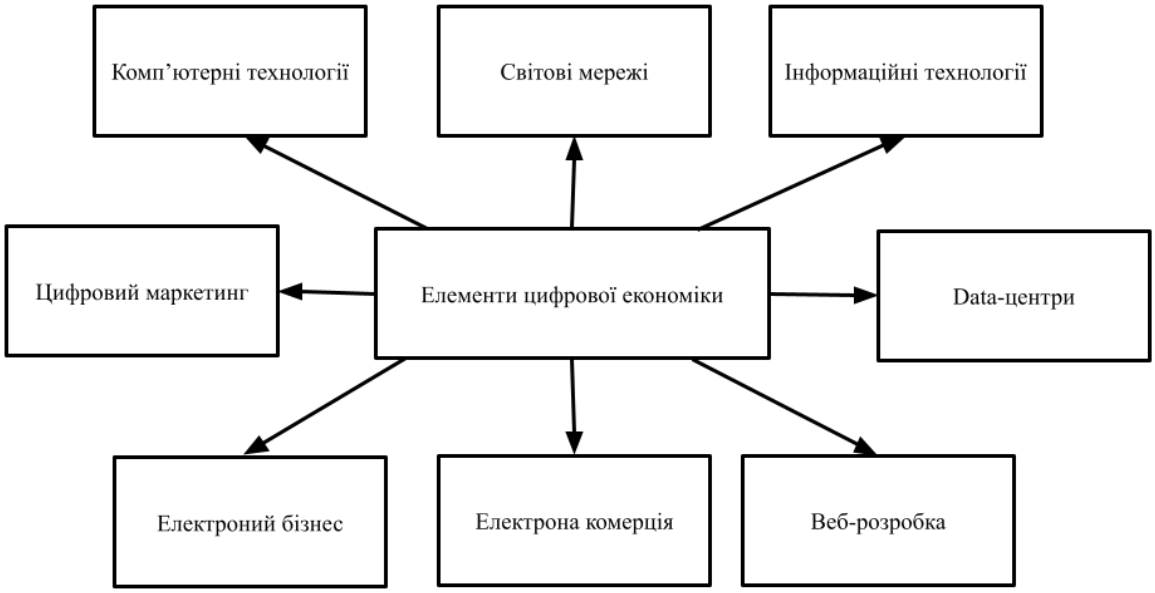


Рисунок 1.2 – Елементи цифрової економіки

Цифрова економіка сприяє та здійснює купівлю-продаж товарів і послуг за допомогою автоматизованих Інтернет-транзакцій. Компоненти цифрової економіки:

– використання цифрових технологій, таких як хмарні обчислення, Інтернет речей і кібербезпека;

– кодифікація процесів і використання блокчейнів для смарт-контрактування;

– комерціалізація знань в інформаційні пакети;

– трансформація виробничих і логістичних процесів;

– гіперсполучна сітка окремих осіб, підприємств, структур. В результаті мобільних технологій (4G/5G) та інших нових технологій підключення [17].

На наступному рисунку можна побачити цифрові тренди на 2019 рік.

Рисунок 1.3 – Технології які використовуються у цифровій економіці [18]

Розглянемо сучасні технології цифрової економіки які активно впроваджуються зараз.

Штучний інтелект (ШІ).

Штучний інтелект — це широка область комп'ютерних наук, яка займається створенням інтелектуальних машин, здатних виконувати завдання, для яких зазвичай потрібний людський інтелект.

Ринок IT визначив нові можливості використання ШІ. Суб'єкти бізнесу повинні використовувати цей інструмент для підтримки конкурентоспроможності та розвитку підсистем. Це спонукає країни вступати у технологічні перегони, щоб стимулювати свою економіку, зміцнювати своє геополітичне становище та підвищувати рівень життя своїх громадян.

ШІ найкраще працює, коли він може інтерпретувати, розуміти та вивчати те, що відбувається в ланцюжку, та забезпечувати підтримку прийняття рішень, якого потребують люди. Саме в так званому розширеному

процесі прийняття рішень штучний інтелект може реально вплинути на трансформацію ланцюжка.

Щоб приймати рішення, які справді впливають на трансформацію ланцюжка, людська відповідальність і розсудливість завжди має бути частиною процесу прийняття рішень [19].

Блокчейн. Блокчейн — це загальний незмінний реєстр, що полегшує процес запису транзакцій та відстеження активів у бізнес-мережах. Активи можуть бути матеріальними та нематеріальними. Практично все, що має цінність, можна відстежувати та продавати в мережі блокчейн, що знижує ризик та витрати для всіх учасників.

Ключові елементи блокчейна:

– технологія розподіленого реєстру. Усі учасники мережі мають доступ до розподіленого реєстру та його незмінного запису транзакцій. У цьому загальному реєстрі транзакції реєструються лише один раз, що усуває дублювання зусиль, характерне для традиційних бізнес-мереж;

– незмінний запис. Як тільки транзакція записується до загального реєстру, учасники не можуть змінювати її або втручатися в неї. Якщо запис транзакції містить помилку, вам потрібно буде додати нову транзакцію, щоб скасувати помилку, і тепер обидві транзакції буде видно;

– смарт-контракт. Для прискорення транзакцій набір правил (смарт-контракти) зберігається у блокчейні та виконується автоматично. Смарт-контракт може визначати умови передачі облігації чи включати умови оплати страхування подорожей.

Механізм блокчейну. Коли відбувається кожна транзакція, записується як блок даних. Ці операції є рух матеріальних чи нематеріальних активів. Блоки даних можуть фіксувати вибрану інформацію.

Але інші технології які були впровадженні раніше також є невід'ємною частиною цифрової економіки, наприклад такі технології як великі дані або

«хмарні технології» є дуже важливими, та відіграють особливу роль для переходу бізнеса на новий рівень [20].

Великі дані (Big Data).

Будь-яка дрібниця інформації, яка надходить в Інтернет, обробляється та перетворюється на дані.

Великі дані – це великі обсяги даних, які дуже швидко генеруються із різних джерел. Дані генеруються як людьми, так і машинами, такими як датчики, які збирають інформацію.

Ефективне використання даних також створює можливості для традиційних секторів, таких як транспорт, охорона здоров'я та виробництво. Поліпшення в аналітиці та обробці даних, особливо великих даних, дозволяють:

− перетворювати сектор послуг шляхом створення широкого спектра інноваційних інформаційних продуктів та послуг;

− поліпшувати бізнес-аналітику та підвищувати продуктивність у всіх секторах економіки;

− вдосконалювати дослідження та прискорювати інновації [21].

Хмарні обчислення.

Хмарні обчислення, технологія, що лежить в основі цифрової економіки, продовжують брати на себе дедалі більше робочих навантажень, оскільки цифрова трансформація продовжує проникати у всі сектори бізнесу.

Хмарні обчислення належать до процесу обслуговування, зберігання, управління, обробки, аналізу та захисту даних з використанням мережі інтернет-серверів. Оскільки дані зберігаються у хмарі, а не на фізичних пристроях, підприємства можуть краще управляти адмініструванням, оптимізувати процеси, підвищувати продуктивність, оптимізувати витрати та покращувати цифрове обслуговування клієнтів.

Щоб залишатися конкурентоспроможними та підвищувати цінність підприємства, всі підприємства мають пройти процес цифрової трансформації,

за потреби оновивши стару IT-інфраструктуру до нової. На додаток до впровадження хмарних рішень підприємства мають інтегрувати нові форми технологій, які прискорюють, автоматизують та покращують їхній бізнес. Приклади включають штучний інтелект, машинне навчання, аналітику великих даних та Інтернет речей (IoT). Хмарні обчислення – це рішення для поєднання цих технологій. Ці технології вимагають великих обчислювальних потужностей та дискового простору [22].

Приклад використання та поєднання таких технологій у бізнесі — є розробка компанії Intel. Інтернет речей (IoT) пропонує величезні нові можливості для бізнесу. Використовуючи сімейство процесорів Intel, організації можуть інтегрувати інтелектуальні засоби реального часу, контроль та інтерактивність майже в будь-який процес.

Українські компанії також мають великий потенціал та розвиваються в цих напрямках. Наприклад, компанія «Індасофт-Україна» активно впроваджує інноваційні технології гібридної локальної хмарної архітектури інтернет-орієнтованих систем автоматизації IIoT/IICS та систем MOM/MES для підвищення ефективності виробництва.

1.3.2 Вплив новітніх технологій на цифрове суспільство

Сталий розвиток, за визначенням міжнародної комісії — це «розвиток, який задовольняє потреби нинішнього покоління без шкоди для можливості майбутніх поколінь задовольняти свої власні потреби» [23].

Потреби поколінь є важливою категорією для визначення напрямків сталого розвитку. Існують теорії, які дозволяють класифікувати, відокремлювати різні групи поколінь, серед яких виділяють «цифрове» та «альфа» покоління.

Чому пропонується розглядати «цифрове» та «альфа» покоління?

Цифрове покоління — термін який вживається для людей народжених приблизно між 1996 та 2010 роках, хоча межі в теорії поколінь не є чіткими. «Цифрове» покоління — перше покоління, що повністю народилося в епоху глобалізації та постмодернізму. [24] «Альфа» покоління — люди повністю народжені у XXI столітті. У сфері розваг у дитинстві покоління «альфа» все більше домінують розумні технології. «Цифрове» покоління вже є платоспроможним, а покоління «альфа» це тенденції майбутнього на які потрібно звертати увагу [25].

Особливості «цифрового» покоління:

– кліпове мислення — здатність людини сприймати світ через короткі яскраві образи та послання. Це масиви інформації сприймаються фрагментами завдяки образам, ярких красок. Людина сприймає навколишню дійсність як послідовність не пов’язаних між собою явищ, а не як цілісну картину. [26] Такому поколінню підходять презентації та картинки, та менше використання тексту. Краще описувати продукцію та послуги фактами та цифрами;

– багатозадачність. Багатозадачність — можливість робити декілька справ одночасно. Роблячи якесь завдання, люди можуть прослуховувати музику, чи онлайн курс. Працювати та відповідати на повідомлення тощо;

– сильна прив'язка до гаджетів. Цифрове покоління активно використовує діджитальні об'єкти. Це не лише цифрові пристрої, а і сторінки в соцмережах де спілкуються люди, створюються онлайн-магазини;

– суттєве зменшення тривалості уваги. Вчені стверджують, що цифрове покоління скоротило тривалість уваги до 8 секунд. Вони не можуть зосередитися на чомусь більший час. Представники цього покоління народилися у світі, можливості якого великі, а часу на все не вистачає. Саме тому вони адаптувалися до необхідності дуже швидко оцінювати та аналізувати величезні обсяги інформації. Масив інформації повинен бути

розрахований виключно на емоційне сприйняття фрагментів запропонованого контенту. У мобільних додатках та сервісах вони покладаються секції вкладення (меню), де зібрано актуальну інформацію.

Перераховані особливості призвели не лише до зміни поведінки цифрового покоління, але й до суттєвих змін в самому середовищі існування та взаємодії людей.

Зокрема, можна спостерігати суттєві трансформації в маркетинговій діяльності, яка враховує ці нові тенденції та використовує їх для створення нових методів впливу:

Контекстна реклама — це онлайн-просування, реклама яка відображається на основі вмісту сторінки або запиту, введеного в пошуковій системі. Таку рекламу бачать користувачі, інтереси яких збігаються з рекламним продуктом або послугою.

Нативна реклама — ненав'язливий спосіб привернення уваги до продукту, сприймається користувачами як корисний контент. Така реклама може працювати як показ товару або послуги декілька днів підряд без натяку що це є реклама. Така модель показу залишає тригери залишається у свідомості людини.

Таргет, таргетована реклама. Часто людям стало здаватися що телефони їх «прослуховують», тому що з’являється реклама товарів які шукалися до цього, так працює таргетована реклама. Таргетована реклама – показ користувачам реклами в соціальних мережах, програмах і на сайтах. Такі оголошення відповідають певним параметрам – «точкам прицілювання»: стать, вік, освіта, геолокація, поведінка. Таргетована реклама спрямована на певну цільову аудиторію. Але як реклама розуміє кому потрібно надати цю рекламу? Під час реєстрації на будь-якому сервісі, залишаються дані про відвідувачів (вік, стать, вподобання), іншим важливим фактором є збираємі файли cookie.

Файл cookie — це невеликий фрагмент тексту, який надсилається у браузер із веб-сайту, який відвідується. З їх допомогою сайт запам'ятовує інформацію про ваш візит. Файли cookie та інші аналітичні технології допомагають збирати дані, які допомагають послугам визначати, як ви взаємодієте з певними продуктами. Ця статистика дозволяє власникам послуг покращувати вміст і розробляти функції, які підвищують зручність використання.

Оскільки, цифрове покоління є багатозадачними, тому дуже часто шукають товари в інтернеті не виходячи з дому. Дуже популярним є створення інтернет-магазинів (навіть якщо є фізичний магазин), та створення чат-ботів. Чат-бот допомагає швидко, без втручання менеджера створити замовлення. Багатозадачність також означає що люди цього покоління можуть залучати декілька органів сприйняття. Зараз з’явилося багато безкоштовних онлайн курсів (Massive Open Online Course) які вдосконалюють як tech, так і soft skills, розробники цих курсів пропонують як альтернативу — подкасти, ідеальний варіант для зайнятої людини. Подкаст — вид аудіо або відеоконтенту, коли один або кілька ведучих обговорюють різні теми.

Виклики останнього часу, такі як коронавірус, зміна безпекового ландшафту, інтенсифікують використання технологій цифрового покоління. З'являються нові тенденції взаємодії в професійному середовищі та в громадських сервісах, наприклад за допомогою хмарних технологій зручно працювати на відстані. Також зручним є те, що багато державних послуг змогли перенестися у цифровий вигляд, наприклад: ДІЯ, Helsi, електронний документообіг, ЦНАП тощо.

На відміну від цифрового покоління, «альфа» покоління складно схарактеризувати достатньо вичерпано. Це пояснюється тим, що вони їх модель поведінки знаходиться на стадії формування. Але можна зробити певні припущення щодо ролі технологій в їхньому житті.

Покоління «альфа» мають достатньо сильний вплив на батьків та навколишній світ.

Останні представники покоління народяться приблизно 2025-го, їх буде майже 2 млрд. Вплив технологій та гаджетів на їхнє життя буде досить сильним. Їх іграшками є роботи, іграшки зі штучним інтелектом, гаджеті з різними додатками.

Особливості покоління «альфа»:

– відсутність розвинутого соціального життя. «Альфа» діти мають не дуже розвинене соціальне життя в суспільстві, але практично у кожного є обліковий запис у соцмережах попри юний вік. Деякі облікові записи достатньо на високому рівні, що дозволяє дітям заробляти з раннього віку. Вони мають достатньо кишенькових грошей, щоб робити самостійні покупки, що вже зараз стає предметом для роздумів серед маркетологів;

– наявність доступу до безлічі інформації. Покоління «альфа» має великий доступ до всілякої інформації з самого раннього дитинства, тому у них добре розвинена навичка фільтрації інформації на потрібну та непотрібну. Досить велика кількість викладачів помічають, що такі діти шукають практичне застосування до тем, які викладають, і шукають зв'язок із реальним життям та можливістю заробітку на цьому. Наприклад, багато розробників ігор “наймають” дітей для просування їхньої продукції, тому час на освіту вони витрачають менше ніж те саме «цифрове» покоління. Їм будуть потрібні нові програми та методи навчання, які можуть їх зацікавити. Більшість покоління займатиметься самоосвітою і перейде на онлайн навчання;

– вміння формувати чітко визначену мету. У них раніше, ніж у «цифрового» покоління, формуватимуться чіткі посили, що потрібно вивчати: це наука, технології. Покоління «альфа» займеться роботою, якої ще не існує. Вже зараз створюється велика кількість нових професій в Інтернеті. Люди без особливої освіти створюють нові курси на прикладах свого досвіду, і ці курси досить успішно продаються серед молоді;

– зростання тривалості життя. «Альфа» покоління хвилюватиметься за здоров'я та глобальні проблеми. Також їх цікавитимуть питання космосу та його простору [27].

Прикладом технологій які вже виходять на ринок та можуть зацікавити покоління «альфа» — є розробки Ілона Маска. Такі розробки як PayPal (онлайн платежі), SpaceX – приватна компанія яка займається створенням космічних кораблів, Tesla – електромобілі, належать йому та можуть достатньо зацікавити майбутнє покоління. Для відокремлення особливостей, був розроблений рис.1.4.

Рисунок 1.4 – Особливості «цифрового» та «альфа» поколінь

У підсумку можна сказати що покоління модернізується разом зі всесвітом і саме люди впливають на ці зміни. Кожне з поколінь є в деякому розумінні удосконаленням попереднього, але також бувають і “втрати”, наприклад в соціальному житті. також приділяти увагу Спостереження за потребами та змінами поколінь допомагає: власникам бізнесу, маркетологам, аналітикам, зробити певні висновки для покращення своїх продуктів або послуг. Теорія поколінь є одним із важливих критеріїв яким необхідно створюючи свою модель удосконалення пропозиції товару чи послуги на ринку.

Висновки до першого розділу

В першому розділі були розглянуті теоретичні засади побудови безпеки підприємства, та складові безпеки підприємства. Фінансова безпека поділяється на: економічну, інформаційну, кадрову, репутаційну, правову, кадрову.

Фінансовий механізм є невід’ємною складовою безпеки підприємства, так як впливає на майже всі розділи безпеки підприємства. Об'єктом управління фінансового механізму є грошовий оборот підприємства, що є безперервним рухом грошових надходжень і платежів за розрахунковими та іншими рахунками підприємства.

Також в першому розділі проілюстровано розвиток цифрової економіки як нові можливості та нові виклики для фінансового механізму підприємства; зроблено аналіз сучасних технологій для забезпечення фінансової безпеки в умовах цифрової економіки. Згідно з цього аналізу, можна зробити висновок, для того щоб залишатися конкурентоспроможними та забезпечувати безпеку на багатьох рівнях, а також підвищувати цінність підприємства, всі підприємства мають пройти процес цифрової трансформації, за потреби оновивши стару IT-інфраструктуру до нової. Підприємства мають інтегрувати нові форми технологій, які прискорюють, автоматизують та покращують їхній бізнес. Приклади включають штучний інтелект, машинне навчання, аналітику великих даних та Інтернет речей (IoT). Хмарні обчислення – це рішення для поєднання цих технологій. Ці технології вимагають великих обчислювальних потужностей та дискового простору.

Під час вирішення впровадження новітніх технологій у бізнес, необхідно також звертати увагу на теорію поколінь. Спостереження за потребами та змінами поколінь допомагає: власникам бізнесу, маркетологам, аналітикам, зробити певні висновки для покращення своїх продуктів або послуг.

2 АНАЛІЗ ДІЯЛЬНОСТІ ТА ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ КОМПАНІЇ «CISCO»

2.1 Характеристика діяльності та контуру управління компанії «Cisco»

Cisco Systems — американська транснаціональна корпорація та найбільший у світі виробник мережевого обладнання, призначеного для забезпечення мереж віддаленого доступу, служб безпеки, мереж зберігання даних, маршрутизації та комутації, а також бізнес-зв'язку IP-комунікацій.

Основні продукти та технології компанії:

− інфраструктурні платформи – комутатори, маршрутизатори, продукти центрів обробки даних і бездротові мережі. Разом їхні функції забезпечують роботу мережі, передачу та зберігання інформації;

− додатки – це бонуси, пов'язані з програмним забезпеченням. Вони використовують різні платформи: мережу, дата-центр;

− безпека. Це включає інноваційні продукти з уніфікованим керуванням загрозами для захисту від загроз. Компанія надає продукти для захисту мережі, хмари та електронної пошти, ідентифікації та керування доступом;

− інші пропозиції включають відеотехнології, архітектуру трансформації бізнесу тощо.

«Cisco» розробляє та продає широкий спектр технологій, які забезпечують роботу Інтернету, інтегрує платформи в мережі, безпеку, співпрацю, програми та хмару. Ці платформи розроблено, щоб допомогти клієнтам керувати більшою кількістю користувачів, пристроями та речами, які підключаються до їхніх мереж. Це дозволяє надавати клієнтам високобезпечну інтелектуальну платформу для цифрового бізнесу.

Стратегія «Cisco».

Допомагайте клієнтам підключатися, захищати та автоматизувати , щоб

пришвидшити свою цифрову гнучкість у світі, орієнтованому на хмару.

Стратегічні принципи. Щоб реалізувати стратегію та відповідати пріоритетам клієнтів, компанія зосереджується на наступних шести стратегічних напрямах:

– безпечні, гнучкі мережі — мережеві рішення з вбудованою простотою, безпекою, гнучкістю та автоматизацією;

– оптимізований досвід роботи з програмами — можливість увімкнути більшу швидкість, гнучкість і масштаб програм, які працюють у хмарі;

– гібридна робота — безпечніше робоче місце та досвід співпраці для гібридної робочої сили;

– інтернет для майбутнього — трансформація підключення, ефективно задовольняючи постійно зростаючий попит на низьку затримку та вищу швидкість;

– наскрізна безпека — створення простих, інтегрованих та високоефективних наскрізних рішень безпеки, які надаються локально або в хмарі;

– можливості на межі — розробка нових можливостей для розподіленого світу, покращуючи досвід розробників і розширюючи корпоративні та операторські мережі.

Мета компанії Cisco – створити інклюзивне майбутнє для всіх. Компанія прагне прокладати шлях, надихати на зміни, дивитися на світ очима інших і долати виклики нерівності, щоб створити нові можливості.

Технологічні мегатренди які застосовує компанія:

– впровадження хмарних технологій (для забезпечення безпеки також);

– перехід до гібридної роботи;

– перехід на 5G і Wi-Fi 6;

– програми та робочі навантаження наближаються до користувачів.

Cisco веде свій бізнес у всьому світі (рис 2.1). Бізнес організований у таких трьох географічних сегментах: Америка; Європа, Близький Схід і Африка (EMEA); і Азіатсько-Тихоокеанський регіон, Японія та Китай (APJC).

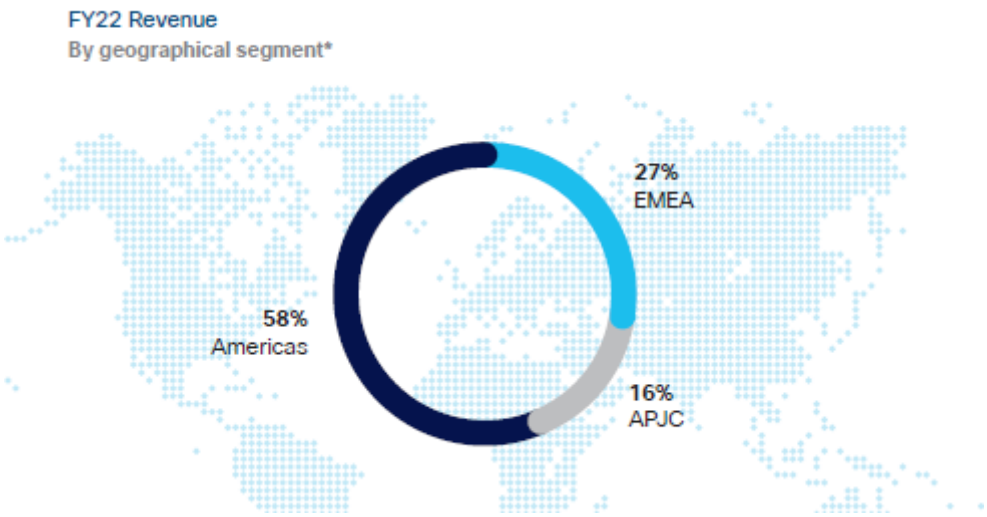


Рисунок 2.1 – Географічний розподіл продажу за 2022 р.

Продукти та технології згруповані в такі категорії: безпечні, гнучкі мережі; інтернет для майбутнього; співпраця; наскрізна безпека; оптимізований досвід застосування; та інші продукти. Окрім пропозицій продуктів, компанія надає широкий спектр пропозицій послуг, включаючи послуги технічної підтримки та розширені послуги. Серед клієнтів — компанії будь-якого розміру, державні установи, уряди та постачальники послуг, у тому числі великі веб-провайдери.

Загальні пропозиції щодо обслуговування та підтримки об’єднані в одну організацію Customer Experience, яка відповідає за наскрізну взаємодію з клієнтами.

Послуги підтримки та технічного обслуговування допомагають клієнтам забезпечити ефективну роботу їхніх продуктів, доступність і переваги найновішої системи та прикладного програмного забезпечення. Ці послуги допомагають клієнтам захистити свої інвестиції в мережу, керувати ризиками та мінімізувати час простою систем, на яких працюють критично важливі

програми. Ключовим прикладом є Cisco Smart Services, яка використовує інтелектуальні дані з встановленої бази продуктів і підключень клієнтів для захисту та оптимізації інвестицій у мережу для клієнтів і партнерів.

Для розвитку інновацій «Cisco» застосовує новітні технології, такі як машинне навчання та розширена аналітика, щоб керувати мережевими можливостями та покращувати їх. Ці пропозиції мережевих продуктів розроблені, щоб допомогти клієнтам виявляти загрози кібербезпеці навіть у зашифрованому трафіку. Таким чином, «Cisco» створила, єдину мережу, яка розроблена для забезпечення безпеки, а також допомагає зберегти конфіденційність.

Окрім цього, компанія «Cisco» має свою мережеву академію та пропонує освітні послуги підготовки майбутніх фахівців IT-індустрії. Мережева академія «Cisco» — це міжнародна освітня програма в області IT і кібербезпеки, яка об'єднує партнерські навчальні заклади по всьому світу. Це найбільша і сама довгострокова програма корпоративної соціальної відповідальності «Cisco» [28].

2.2 Аналіз основних показників діяльності компанії «Cisco»

У процесі формування аналізу використовується баланс (звіт про фінансовий стан), звіт про фінансові результати (звіт про прибутки і збитки), інші елементи звітності компанії «Cisco». Економічні дані, фінансові індикатори та інша інформація, що надається компанією «Cisco», використовуються для забезпечення зважених висновків про поточний фінансовий стан і ефективність роботи компанії. В якості періоду дослідження використовується 2020-2022 рр. Об'єктами розгляду є окремі напрямки і господарські процеси, елементи в своїй сукупності господарської діяльності

підприємства. Сутність показників висловлює економічну суть та їх конкретне значення (табл.2.1) [29].

Загальний дохід зріс на 3% порівняно з 2021 фінансовим роком. Серед загального доходу дохід від продуктів збільшився на 6%, а дохід від послуг зменшився на 2%.

Таблиця 2.1 – Звіт про доходи компанії «Cisco» за період 2020-2022рр (млн. USD)

Період до:	2022 30/07	2021 31/07	2020 25/07	2019 27/07
Загальний дохід	51 557	49 818	49 301	51 904
Виторг	51 557	49 818	49 301	51 904
інші прибутки	-	-	-	-
Вартість доходів	19 309	17 924	17 618	19 238
Валовий прибуток	32 248	31 894	31 683	32 666
Разом Операційні витрати	37 532	36 053	35 179	37 685
Продаж/загальні/адміністративні Витрати, всього	11 136	11 365	11 073	11 439
Дослідження та розробки	6 774	6 549	6 347	6 577
Амортизація	-	215	141	150
Відсоткові витрати (доходи)	-360	-434	-585	-
Незвичайні витрати (доходи)	-	906	477	281
Інші операційні витрати, всього	673	649	726	-
Операційні доходи	14 025	13 765	14 122	142 19
Відсоткові доходи (витрати), не-операційні, нетто	-	509	467	366
Прибуток (збиток) від продажу активів	466	345	141	-
Інші доходи, нетто	-918	158	11	-14
Чистий прибуток до податків	14 477	13 262	13 970	14 571
Відрахування на сплату податків	2 665	2 671	2 756	2 078
Чистий дохід після сплати податків	11 812	10 591	11 214	12 493
Частка меншості	-	-	-	-
Акції у філіях	-	-	-	-
Перерахунок згідно із загальноприйнятими принципами бухгалтерського обліку США	-	-	-	-
Чистий прибуток до вирахування надзвичайних статей	11 812	10 591	11 214	12 493

Продовження таблиці 2.1

Період до:	2022 30/07	2021 31/07	2020 25/07	2019 27/07
Надзвичайні статті	-	-	-	-872
Чистий прибуток	11 812	10 591	11 214	11 621
Коригування чистого прибутку	-	-	-	-
Прибуток за звичайними акціями, за винятком надзвичайних статей	11 812	10 591	11 214	12 493

У 2022 фінансовому році загальний дохід від програмного забезпечення залишився незмінним і становив 15,1 мільярда доларів США за всіма продуктами та послугами. У загальному доході від програмного забезпечення дохід від підписки зріс на 3%.

Загальний валовий прибуток зменшився на 1,5 відсотки. Валова рентабельність продукту зменшилася на 2,1 відсотки, в основному через збільшення витрат, пов'язаних з обмеженнями поставок, і, меншою мірою, асортиментом продукції, частково компенсоване сприятливими цінами. Як відсоток від доходу, дослідження та розробки, продажі та маркетинг, а також загальні й адміністративні витрати разом зменшилися на 1,3 відсотки. Операційний дохід у відсотках від виручки зріс на 1,3 проценти. Розбавлений прибуток на акцію збільшився на 13%, завдяки збільшенню чистого прибутку на 12% і зменшенню розбавленої кількості акцій на 44 мільйони акцій. Графічно ці дані зображено на рис. 2.2.

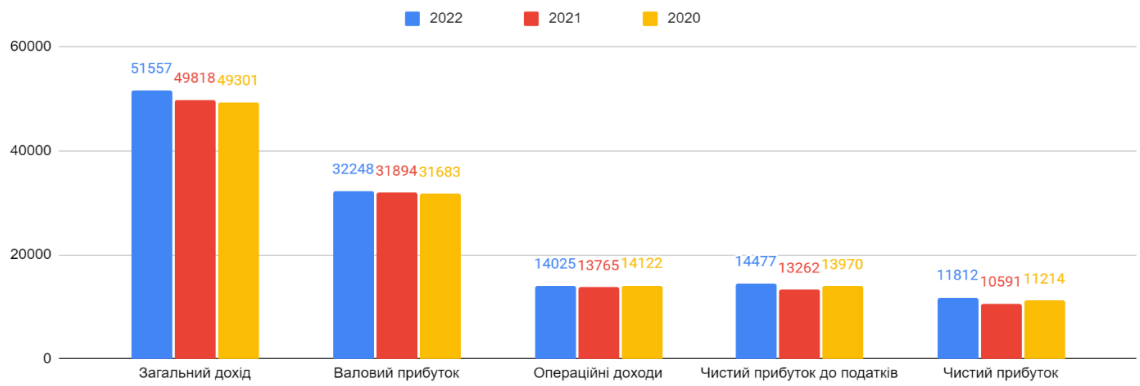


Рисунок 2.2 – Показники доходу та прибутку за 2020-2022рр.

Згруповані активи та зобов’язання можна подивитись на рис. 2.3.

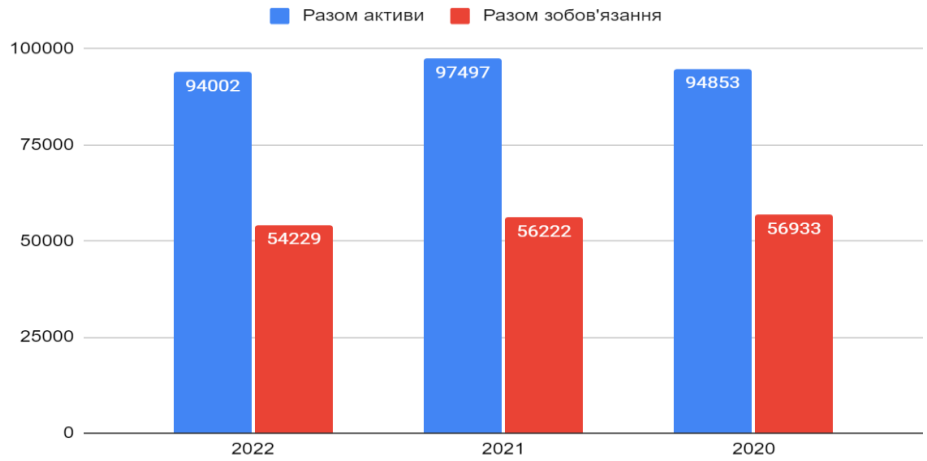


Рисунок 2.3 – Разом активи та зобов’язання за 2020-2022рр.

Дохід згідно з географічних сегментів (табл.2.2). Дохід від Америки зріс на 0,7 мільярда доларів США, дохід у регіоні EMEA збільшився на 0,8 мільярда доларів США, а дохід у сегменті APJC збільшився на 0,3 мільярда доларів США.

Таблиця 2.2 – Дохід від продукту за географічним сегментом за період 2020-2022рр. (в млн. USD, окрім відсотків)

Дохід від продукту:	30.07.2022	31.07.2021	25.07.2020	Відхилення в доларах (2022-2021)	Відхилення у відсотках (2022-2021)
Америки	21 620	20 688	21 006	932	5%
Відсоток доходу від продукту	56,90%	57,50%	58,40%		
EMEA	10 545	9 805	9 647	740	8%
Відсоток доходу від продукту	27,70%	27,20%	26,80%		
APJC	5 854	5 521	5 326	333	6%
Відсоток доходу від продукту	15,40%	15,30%	14,80%		
Всього	38 018	36 014	35 978	2,004	6%

Дохід від продукції в сегменті Америки зріс на 5%. Збільшення доходу від продукту було зумовлене зростанням на ринках постачальників послуг, комерційному та корпоративному ринку, частково компенсованим падінням ринку державного сектора.

Збільшення доходу від продукту в сегменті EMEA на 8% було зумовлене зростанням на комерційних, корпоративних ринках і ринках постачальників послуг. Ринок державного сектора залишався без змін. З точки зору країни дохід від продукту зріс на 14% у Великобританії та на 9% у Німеччині, частково компенсований зниженням на 3% у Франції.

Дохід від продукції в сегменті APJC зріс на 6%, завдяки зростанню на комерційному та корпоративному ринках, частково компенсованому падінням на ринках постачальників послуг і державному секторі. З точки зору країни дохід від продукту зріс на 18% у Китаї та на 10% в Австралії, частково компенсований падінням на 9% у Японії та 1% в Індії.

Дохід від продукту за категоріями. З точки зору категорії продукту, загальний дохід від продукту зріс на 6% у порівнянні з минулим роком завдяки зростанню доходу в Secure, Agile Networks на 5%; Інтернет для майбутнього 17%; Наскрізна безпека 9% і оптимізована робота додатків 11%; частково компенсується зниженням доходу від продуктів у Collaboration на 5%.

У наведеній нижче таблиці подано доходи від продукту за категоріями (у мільйонах, крім відсотків):

Таблиця 2.3 – Дохід від продукту за категоріями за період 2020-2022рр. (в млн. USD, окрім відсотків)

Дохід від продукту за категоріями	Роки			2022 порівняно 2021		2021 порівняно 2020	
	30.07. 2022	31.07. 2021	25.07. 2020	Відхилення в доларах	Відхилення у відсотках	Відхилення в доларах	Відхилення у відсотках
Безпечні гнучкі мережі	23 829	22 722	23 265	1 107	5%	-543	-2%
Інтернет для майбутнього	5 278	4 514	4 18	764	17%	334	8%
Співпраця	4 472	4 727	4 823	-255	-5%	-96	-2%

Продовження таблиці 2.3

Дохід від продукту за категоріями	Роки			2022 порівняно 2021		2021 порівняно 2020	
	30.07. 2022	31.07. 2021	25.07. 2020	Відхилення в доларах	Відхилення у відсотках	Відхилення в доларах	Відхилення у відсотках
Наскрізна безпека	3 699	3 382	3,158	317	9%	224	7%
Оптимізований досвід застосування	729	654	524	75	11%	130	25%
Інші продукти	11	15	28	-4	-29%	-13	-47%
Всього	38 018	36 014	35 978	2 004	6%	36	—%

У наступній таблиці представлено валову рентабельність продуктів і послуг:

Таблиця 2.4 – Валовий прибуток за період 2020-2022рр. (в млн. USD, окрім відсотків)

	Сума			Відсоток		
Валовий прибуток	30.07.2022	31.07.2021	25.07.2020	30.07.2022	31.07.2021	25.07.2020
Продукт	23,204	22,714	779	61,0%	63,1%	63,3%
Сервіс	9,004	9,18	8,904	66,8%	66,5%	66,8%
Разом	32,248	31,894	683	62,5%	64,0%	64,3%

Валова рентабельність продукту зменшилася на 2,1 відсотки в основному через негативний вплив на продуктивність, головним чином зумовлений збільшенням витрат, пов’язаних з обмеженнями поставок на вантажні перевезення, експедиціями та вищими витратами на компоненти та товари. Ці наслідки були частково компенсовані вигідною ціною. Вигода, яку можна побачити в результаті сприятливого ціноутворення, була в основному зумовлена підвищенням цін, здійсненим у 2022 фінансовому році, щоб частково компенсувати збільшення витрат на компоненти та товари, витрати на транспортування та логістику через обмеження поставок.

Розрахуємо основні фінансові коефіцієнти згідно балансу Додаток А.

Для розрахунку коефіцієнтів ліквідності та рентабельності потрібно скористатися формулами наведеними в табл. 2.5 та табл. 2.6.

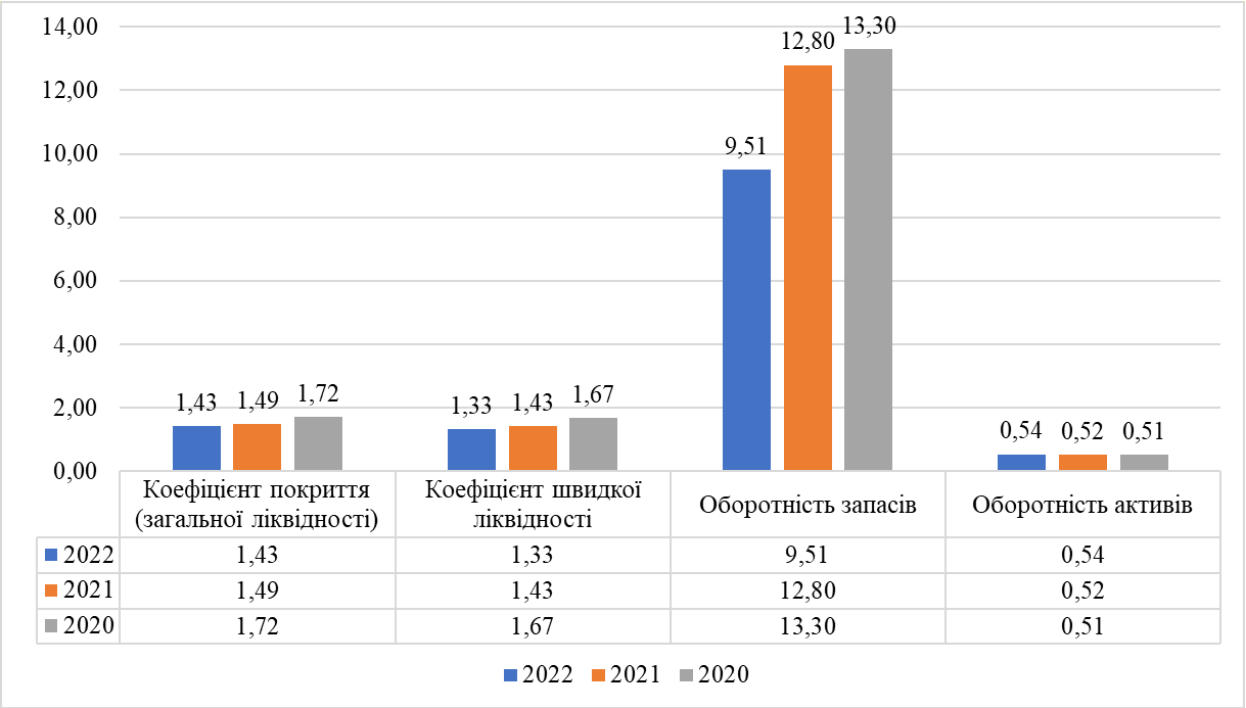
Таблиця 2.5 – Показники ліквідності та платоспроможності

Показники ліквідності та платоспроможності	Формула для розрахунку
1. Коефіцієнт покриття (загальної ліквідності)	$Кзл=\frac{Об.А}{ПЗ}$ Нормативне значення Кзл≥2
2. Коефіцієнт швидкої ліквідності	$Кшл=\frac{Об.а-З}{ПЗ}$ Нормативне значення Кшл≥1
3. Оборотність запасів	$Коз=\frac{СРП}{СВЗ}$ Нормативне значення Коз≥8
4. Оборотність активів	$Коа=\frac{ОП}{ССА}$ Нормативне значення – Коа>1
Об.А – оборотні активи; ПЗ – поточні зобов'язання; З – запаси; ГК – грошові кошти та еквіваленти СРП – собівартість реалізованої продукції СВЗ – середньорічна вартість запасів ОП – обсяг продажу (річний оборот компанії) ССА – середні сумарні активи.	

Таблиця 2.6 – Показники рентабельності

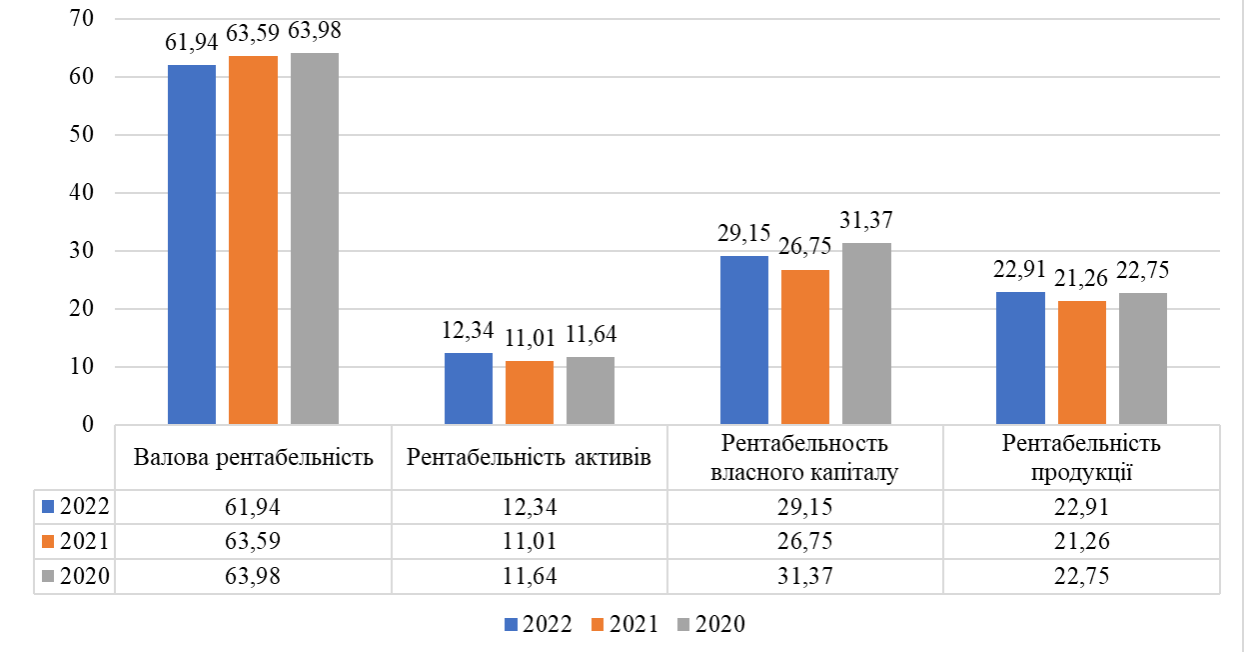
Показники рентабельності	Формула для розрахунку
1. Валова рентабельність	$Рв=\frac{ВП}{ЧВ}$ Нормативне значення Рв>0,15
2. Рентабельність активів	$Ра=\frac{ЧП}{ВБ}$ Нормативне значення Ра>0,14
3. Рентабельність власного капіталу	$Рк=\frac{ЧП}{ВК}$ Нормативне значення Рвк>0,2
4. Рентабельність продукції	$Рп=\frac{ЧП}{ЧВ}$ Нормативне значення Рп>0,15
ВП - валовий прибуток; ЧВ – чиста виручка; ЧП – чистий прибуток; ВБ – валюта балансу; ВК – власний капітал.	

Розрахуємо коефіцієнти та побудуємо графіки за допомогою табличного редактора «Excel». Дані можна побачити на рис. 2.4 та рис. 2.5.



	Коефіцієнт покриття (загальної ліквідності)	Коефіцієнт швидкої ліквідності	Оборотність запасів	Оборотність активів
2022	1,43	1,33	9,51	0,54
2021	1,49	1,43	12,80	0,52
2020	1,72	1,67	13,30	0,51

Рисунок 2.4 – Розраховані коефіцієнти ліквідності за 2020-2022рр.



	Валова рентабельність	Рентабельність активів	Рентабельность власного капіталу	Рентабельність продукції
2022	61,94	12,34	29,15	22,91
2021	63,59	11,01	26,75	21,26
2020	63,98	11,64	31,37	22,75

Рисунок 2.5 – Розраховані коефіцієнти рентабельності за 2020-2022рр.

Згідно цих коефіцієнтів можна зробити висновок, що компанія має високоефективний підхід так як всі коефіцієнти знаходяться у нормі. У 2021 році економічні показники компанії менше ніж у 2020, компанія обумовлює

це ситуацією з пандемією. Але, не дивлячись на важку ситуацію в макроекономічному плані, у 2022 році компанія підвищила деякі свої показники, хоча потрібно звернути увагу на коефіцієнти ліквідності та валову рентабельність.

Компанія забезпечила зростання загального доходу та високу прибутковість у складних умовах, на які вплинули значні обмеження поставок, зростання витрат на компоненти та пов'язаних із цим витрат. Як і раніше компанія зосереджена на впровадженні інновацій у технології, щоб допомагати клієнтам здійснити цифрову трансформацію. На компанію продовжують негативно впливати обмеження поставок, які спостерігаються в усій галузі через дефіцит компонентів. Компанія продовжує прогрес у перетворенні бізнес-моделі, надаючи більше програмного забезпечення та підписок.

2.3 Аналіз технологій забезпечення фінансової безпеки компанії «Cisco»

«Cisco» є одним з лідерів постачання програмного забезпечення для безпеки. Зі стрімким розвитком сучасних програм і більш розподіленим робочим середовищем захист підприємства став складнішим і важчим для клієнтів. Кожній організації потрібні нові або вдосконалені архітектури безпеки для захисту від зростаючих кібератак. Стратегія безпеки зосереджена на створенні простої та ефективної архітектури кібербезпеки, що поєднує мережеві, хмарні та кінцеві рішення, які визнають критичну важливість конфіденційності даних.

Компанія «Cisco» інвестує значні ресурси в портфоліо безпеки, зосереджене на хмарних пропозиціях, виявленні загроз на основі штучного інтелекту та наскрізних архітектурах безпеки. Cisco Security Cloud розроблено

як найбільш відкрита наскрізна платформа безпеки в гібридних багатохмарних середовищах, яка також мінімізує поверхню атак і автоматизує політики безпеки в середовищі організації. Компанія також надає уніфіковані можливості виявлення та реагування за допомогою Cisco SecureX, хмарної платформи, яка є вбудованою платформою, яка поєднує портфоліо Cisco Secure та інфраструктуру клієнтів. Також компанія, нещодавно анонсувала нові пропозиції, спрямовані на захист операцій клієнтів за допомогою Talos On-Demand, що дозволяє проводити спеціальні дослідження середовища загроз, і Secure Cloud Analytics, яка використовує мережу як датчик для виявлення загроз у мережевій інфраструктурі, в приватних і публічних хмарах.

Так само компанія не тільки пропонує такі технології, а й активно використовує їх всередині, про це свідчить два звіти компанії, де вони висловлюються з приводу ризик-менеджменту та «Як Cisco масштабує безпечну віддалену роботу» [29,30].

З наглядом ради директорів «Cisco» – реалізовані практики, процеси та програми, призначені для допомоги в управлінні ризиками, яким піддається компанія.

Кібератаки, витік даних або зловмисне програмне забезпечення можуть порушувати роботу, зашкодити операційним результатам і фінансовому стану, а також шкодити репутації чи іншим чином матеріально шкодити бізнесу; кібератаки чи витоки даних клієнтів або в мережах сторонніх постачальників, або в хмарних службах, може призвести до претензій відповідальності проти компанії.

Керівництво «Cisco» впровадило програму ERM, якою керує «Cisco», її функція – внутрішнього аудиту, щоб ідентифікувати, оцінювати ризики, контролювати та управляти ними. Структура програми ERM включає в себе як робочий комітет ERM, який фокусується на управлінні ризиками теми та виконавчий комітет ERM що складається з членів дирекції.

Операційний комітет ERM проводить глобальні аналізи ризиків і забезпечує регулярне оновлення ERM виконавчий комітет.

«Cisco» масштабує безпечну віддалену роботу. Усі співробітники, підрядники та партнери, які використовують IT-додатки «Cisco», розміщені в центрах обробки даних або філіях, мають доступ до VPN. Вони встановлюють Cisco AnyConnect Secure Mobility Client на своїх ноутбуках і мобільних пристроях. Віддалені працівники, які працюють повний робочий день, мають віртуальний офіс Cisco налаштування, що включає апаратну службу VPN.

Співробітники можуть підключатися до VPN зі своїх корпоративних ноутбуків або особистих планшетів чи смартфонів, зареєстрованих у Cisco IT.

Коли співробітники відвідують веб-сайти, хмарний сервіс Umbrella блокує зловмисні домени, IP-адреси та хмарні додатки до встановлення з’єднання. Захист на рівні DNS допомагає запобігти зловмисному програмному забезпеченню, фішингу та програмам-вимагачам.

З 2020 року компанія спростила дослідження безпеки та пошук загроз, активувавши функцію AMP під назвою Orbital Advanced Search. Це дозволяє переглядати всі пристрої співробітників у певний момент часу, щоб виявити загрози. Команда реагування на інциденти також використовує Orbital, щоб швидко знаходити першопричину інцидентів. Чим швидше знайдена першопричина, тим швидше є змога усунути й тим коротшим буде ризик.

Висновки до другого розділу

В другому розділі проведений аналіз компанії «Cisco». Cisco Systems — американська транснаціональна корпорація та найбільший у світі виробник мережевого обладнання, призначеного для забезпечення мереж віддаленого

доступу, служб безпеки, мереж зберігання даних, маршрутизації та комутації, а також бізнес-зв’язку IP-комунікацій.

Продукти та технології компанії згруповані в такі категорії: безпечні, гнучкі мережі; інтернет для майбутнього; співпраця; наскрізна безпека; оптимізований досвід застосування; та інші продукти. Окрім пропозицій продуктів, компанія надає широкий спектр пропозицій послуг, включаючи послуги технічної підтримки та розширені послуги. Серед клієнтів — компанії будь-якого розміру, державні установи, уряди та постачальники послуг, у тому числі великі веб-провайдери.

В підрозділі 2.2 зроблено аналіз основних показників діяльності компанії «Cisco» за 2020-2022 рр. Основні фінансові коефіцієнти, такі як: рентабельність та ліквідність, дають змогу розуміти що компанія має високоефективний підхід так як всі коефіцієнти знаходяться у нормі. У 2021 році економічні показники компанії менше ніж у 2020, компанія обумовлює це ситуацією з пандемією. Але, не дивлячись на важку ситуацію в макроекономічному плані, у 2022 році компанія підвищила деякі свої показники, хоча потрібно звернути увагу на коефіцієнти ліквідності та валову рентабельність.

Компанія забезпечила зростання загального доходу та високу прибутковість у складних умовах, на які вплинули значні обмеження поставок, зростання витрат на компоненти та пов’язаних із цим витрат. Як і раніше компанія зосереджена на впровадженні інновацій у технології, щоб допомагати клієнтам здійснити цифрову трансформацію. На компанію продовжують негативно впливати обмеження поставок, які спостерігаються в усій галузі через дефіцит компонентів. Компанія продовжує прогрес у перетворенні бізнес-моделі, надаючи більше програмного забезпечення та підписок.

Також переглянута стратегія забезпечення безпеки компанії «Cisco». Керівництво «Cisco» впровадило програму ERM, якою керує «Cisco», її

функція – внутрішнього аудиту, щоб ідентифікувати, оцінювати ризики, контролювати та управляти ними. Структура програми ERM включає в себе як робочий комітет ERM, який фокусується на управлінні ризиками теми та виконавчий комітет ERM що складається з членів дирекції.

Операційний комітет ERM проводить глобальні аналізи ризиків і забезпечує регулярне оновлення ERM виконавчий комітет. З 2020 року компанія спростила дослідження безпеки та пошук загроз, активувавши функцію AMP під назвою Orbital Advanced Search. Це дозволяє переглядати всі пристрої співробітників у певний момент часу, щоб виявити загрози. Команда реагування на інциденти також використовує Orbital.

3 УДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

3.1 Напрямки удосконалення системи фінансової безпеки підприємства в умовах цифрової економіки

В умовах економічної та політичної нестабільності функціонування підприємств значною мірою залежить від обґрунтованих і виважених управлінських рішень та ефективної системи організації діяльності. Через відсутність чіткого напряму розвитку та якісної стратегії управління розвитком вітчизняним підприємствам важко вирішити ці завдання, що призводить до зниження фінансової стійкості, потенціалу та конкурентоспроможності підприємств.

На сучасному етапі розвитку української економіки умови діяльності вітчизняних підприємств є, очевидно, складними. Ефективність діяльності суб'єкта господарювання залежить від його фінансового стану, що потребує врахування питання забезпечення фінансової безпеки бізнесу.

Зараз відбувається четверта промислова революція, з’являються нові технології і у сфері безпеки підприємств. Пропонується проаналізувати ринок послуг в сфері безпеки та досвід компаній які їх впроваджують.

Компанія «Cisco» у 2022 році випустила звіт з приводу найчастіших вірусів які впливають на підприємство. У цьому звіті про видимість безпеки за 2022 рік було опитано 278 фахівців з кібербезпеки, щоб виявити ключові проблеми щодо видимості безпеки, як організації вирішують цю проблему та можливості безпеки, якім організації віддають пріоритету [31].

На питання «З якими проблемами безпеки спеціалісти найбільше стикаються?» — відповіді були наступні: програми-вимагачі (53%) очолюють список після нещодавнього зростання атак програм-вимагачів. Наступною найбільшою проблемою безпеки є перехід до віддаленої роботи та пов’язані з

цим ризики (47%), які з’явилися після пандемії Covid-19. Обмежена видимість кіберзагроз складає (41%) (рис. 3.1).

Рисунок 3.1 – Відповідь на питання «З якими проблемами безпеки спеціалісти найбільше стикаються?» [31]

Все більше підприємств переходять на хмарні технології (52%) вже мають більше чверті робочих навантажень, розгорнутих у хмарі. Очікується, що протягом наступних 12-18 місяців 79% організацій планують розгортати більше чверті робочих навантажень у хмарі.

Відповідь на питання «Який відсоток робочих навантажень зберігається у хмарі ?» наведено на рис. 3.2.

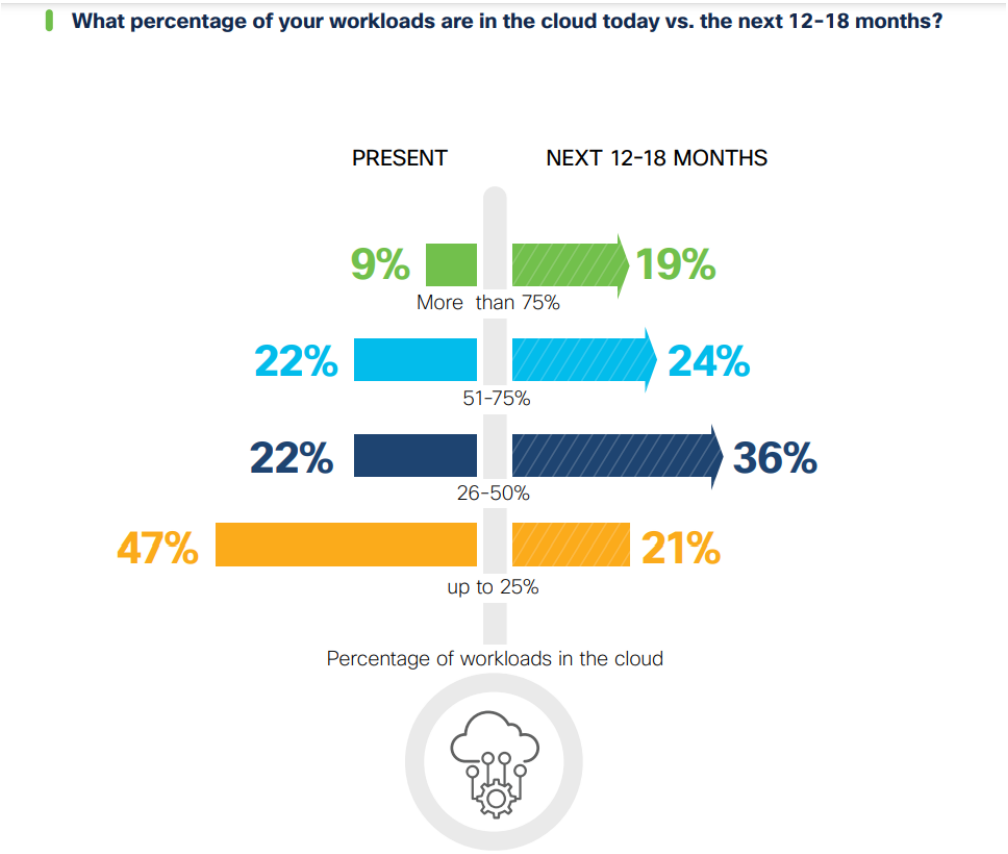


Рисунок 3.2 – Відповідь на питання «Який відсоток робочих навантажень зберігається у хмарі ?» [31]

Прикладом застосування хмарних технологій – можна вважати перевід інформації «ПриватБанку» у хмару.

НБУ дозволив банкам зберігати і обробляти дані «у хмарах» (рішення 8 березня 2022 р.).

«Ми працювали над міграцією наших IT систем з фізичного центру зберігання даних у «хмару» з метою мінімізувати залежність від фізичної присутності комп'ютерного обладнання, розташованого в різних регіонах України, яке могло бути знищено під час війни. У результаті усі основні застосунки ПриватБанку було успішно перенесено у хмарне сховище, щоб забезпечити доступ клієнтів до фінансових послуг у будь-який момент» [32].

Також у звіті компанії «Cisco» було проявлене наступне запитання: «Які продукти впровадили організації, щоб отримати доступ до мережевого трафіку?». Мережевий трафік або трафік даних — це кількість даних, що

переміщуються мережею за певний час. Більшість даних у комп’ютерній мережі інкапсульовано в мережеві пакети, які фактично забезпечують навантаження на мережу.

Брандмауери (програма чи пристрій, що здійснює захист комп'ютерних мереж) очолюють список (74%), за ними йдуть агенти безпеки кінцевих точок(це фізичні пристрої, які підключаються до комп’ютерної мережі й обмінюються з нею інформацією) (62%) і платформи SIEM (збирають інформацію із серверів, контролерів доменів, файрволів та багатьох інших мережевих пристроїв та надають її у вигляді зручних звітів) (58%). Відповідь на питання «Які продукти впровадили організації, щоб отримати доступ до мережевого трафіку?» (рис.3.3).

Рисунок 3.3 – Відповідь на питання «Які продукти впровадили організації, щоб отримати доступ до мережевого трафіку?» [31]

В Україні останнім часом зростають Cashless-розрахунки. НБУ на офіційному сайті продемонстрували аналіз 2021 року по безготівковим розрахункам.

«Обсяг операцій з використанням платіжних карток українських банків склав 7 817,1 млн операцій на суму 5 091,7 млрд гривень. Порівняно з 2020 роком кількість і вартість цих угод зросла приблизно на третину (30,3% і 28,7% відповідно). У 2021 році 9 з 10 операцій будуть безготівковими (90,1% усіх операцій з платіжними картками). Аналіз розподілу видів безготівкових операцій показує, що, як і раніше, найбільше операцій за допомогою карток у 2021 році буде: за обсягом – розрахунки в торговельній мережі – 52,4% (або 3,686 млрд шт.). На них припадає більше чверті (28,4%) усіх безготівкових операцій; за сумою – перекази з картки на картку – 43,6% (або 1352 млрд грн). Їх кількість становить 12,7% (рис.3.4).

Рисунок 3.4 – Розподіл безготівкових операцій з використанням платіжних карток [33]

Таким чином, забезпечення безпеки також потребує і процес безготівкового розрахунку та зберігання грошей компанії.

Проаналізуємо ринок послуг та сервісів з надання безпеки для підприємства в умовах цифрової економіки.

Компанія «Cisco» пропонує вбудовану в середовище хмарну платформу для інтеграції рішень «Cisco» з безпеки з існуючою інфраструктурою підприємства – SecureX. Це комплексний відкритий продукт, що допомагає централізувати всі засоби контролю й помітно підвищити експлуатаційну ефективність систем кібербезпеки за рахунок автоматизації робочих процесів [28].

Компанія Microsoft пропонує – засоби захисту для малого й середнього бізнесу. Це – «Microsoft Defender для бізнесу» та «Microsoft 365 Business преміум».

Defender для бізнесу — це рішення для забезпечення безпеки кінцевих точок (фізичні пристрої, які підключаються до комп'ютерної мережі й обмінюються з нею інформацією), розроблене спеціально для малого та середнього бізнесу (до 300 співробітників). Завдяки цьому рішення для забезпечення безпеки кінцевих точок пристрої компанії краще захищені від програм-шантажистів, шкідливих програм, фішингу та інших загроз.

Microsoft 365 Business Premium – набір продуктів Windows 10 Pro у вигляді Upgrade, Office 365, Enterprise Mobility and Security. Microsoft 365 Business – був спеціально створений для малих і середніх підприємств з числом користувачів до 300 осіб. Містить кращі в своєму класі програми і служби для продуктивної роботи зі складу Office 365 бізнес преміум, а також розширені засоби забезпечення безпеки, які захистять дані і активи вашої компанії на всіх пристроях [34].

Ще однією розробкою є модуль у Oracle Fusion Cloud ERP – Oracle Risk Management. Потрібний для управління ризиками та дотримання вимог щодо відповідності та конфіденційності (SoD, SOX, GDPR тощо). Абоненти Oracle

Risk Management можуть автоматизувати аналіз, моніторинг і контроль безпеки ERP, конфігурацій і транзакцій. Oracle Risk Management використовує сучасну науку про дані та методи штучного інтелекту, щоб допомогти розробити безпечні ролі, вирішити конфлікти SoD, відстежувати конфігурації та виявляти підозрілі транзакції для захисту від шахрайства з платежами та помилок [35].

Таку технологію цифрової економіки як блокчейн, можна також застосувати для забезпечення безпеки підприємства. Технологія блокчейн створює структури даних із властивими їм якостями безпеки. Такі структури ґрунтуються на принципах криптографії, децентралізації та консенсусу, які гарантують довіру транзакцій. У більшості блокчейнів або технологій розподіленого реєстр дані структуровані блоки, кожен з яких містить транзакцію або групу транзакцій. Кожен новий блок пов'язаний з усіма попередніми блоками в криптоланцюжку, що робить підробку практично неможливою. Усі транзакції всередині блоку перевіряються та координуються з використанням механізму консенсусу, щоб гарантувати, що кожна транзакція є правдивою та правильною.

Технологія блокчейн забезпечує децентралізацію за рахунок участі учасників у децентралізованій мережі. Немає єдиної точки відмови, і користувачі не можуть змінювати записи транзакцій.

При створенні корпоративної програми блокчейна важливо враховувати безпеку на всіх рівнях технологічного стеку та те, як здійснюється керування мережею та дозволами. Комплексна стратегія безпеки для корпоративних блокчейн-рішень включає використання традиційних та пропрієтарних засобів контролю безпеки. Елементи управління безпекою, характерні для корпоративних блокчейн-рішень, включають:

- управління ідентифікацією та доступом;
- ключовий менеджмент;
- конфіденційність даних;

– безпечне з'єднання;
– безпека смарт-контрактів
– підтвердження згоди [36].

Також в Україні набуває популярності напрям – «Форензік аудиту». «Форензік аудит» – незалежне розслідування іншими компаніями, використовується для виявлення фінансових порушень та запобігання економічним злочинам бізнесу. Наприклад таку послугу надає компанія – «Revealing Information – юридична компанія». Послуга включає в себе: фінансові розслідування; аналіз і побудову системи внутрішньої безпеки компанії; фінансовий контролінг на аутсорсингу; захист інвестицій / контроль над цільовим використанням грошей; проведення внутрішнього аудиту; використання підходу e-Discovery та ін.

Необхідно розрізняти різницю між аудитом і форензик-перевіркою: аудит покликаний підвищити довіру до фінансової звітності компанії, ключовий момент — операції перевіряються з урахуванням вибірки, тоді як форензик передбачає всебічний аналіз, що стосується як фінансових і юридичних питань, а й усіх нематеріальних аспектів. Він спрямований на запобігання випадкам шахрайства та допомагає мінімізувати ризики вчинення недобросовісних дій, що завдають шкоди компанії [37].

Альтернативним, не схожим на інші, підходом до забезпечення безпеки підприємства, є технологія – «Zero Trust». Вона потребує багато часу для виконання, хоча є новітньою технологією забезпечення безпеки.

Zero Trust – це система безпеки, яка вимагає автентифікації, авторизації та постійних перевірок конфігурації та стану безпеки для всіх користувачів всередині та за межами мережі організації, перш ніж отримувати або підтримувати доступ до програм та даних. Нульова довіра означає відсутність традиційних мережевих обмежень. Мережі можуть бути локальними чи хмарними. Це або об'єднання ресурсів у будь-якому місці з робітниками будь-де, або гібрид.

Реалізація цього фреймворку (програмна платформа, що визначає структуру програмної системи) поєднує передові технології, такі як багатофакторна автентифікація на основі ризиків, захист ідентичності, безпека кінцевих точок нового покоління і надійні технології хмарних робочих навантажень для перевірки посвідчень користувачів або систем, а також доступу до безпеки системи та підтримки. Zero Trust також повинен враховувати шифрування даних, безпеку електронної пошти та перевірку працездатності активів та кінцевих точок перед їх підключенням до програм.

Zero Trust дуже відрізняється від традиційної мережевої безпеки. Традиційний підхід автоматично довіряє користувачам та кінцевим точкам у межах периметра організації, відкриваючи організацію для законних облікових даних, захоплених інсайдерами або зловмисниками, та запобігаючи шахрайським обліковим записам та компрометації. Ви зможете використовувати існуючий обліковий запис. Вона отримує, коли обліковий запис входить усередину

Архітектура з нульовою довірою вимагає від організацій постійного моніторингу та забезпечення наявності у користувачів та їх пристроїв відповідних дозволів та атрибутів. Вам також потрібні політики, які враховують ризики користувачів та пристроїв, а також відповідність вимогам та інші вимоги, які необхідно враховувати, перш ніж дозволяти транзакції. Для цього організації необхідно знати всі сервісні та привілейовані облікові записи та контролювати їх. Загрози та атрибути користувачів можуть змінюватися, тому однієї перевірки недостатньо [38].

Можна зробити висновок, що ринок з надання послуг захисту безпеки підприємств достатньо великий та постійно оновлюється, для того щоб обрати правильний підхід та технологію – необхідно побудувати єдину покрокову систему із забезпечення безпеки підприємства.

3.2 Розробка технологічної складової для системи фінансової безпеки підприємства в умовах цифрової економіки

Проаналізувавши в підрозділі 3.1 удосконалення системи фінансової безпеки підприємства в умовах цифрової економіки– пропонується розробити систему забезпечення фінансової безпеки підприємства з урахуванням цих технологій.

Для плавного переходу підприємства на більш якісне формування фінансової безпеки, пропонується впроваджувати поетапний підхід, який буде поділятися на 4 етапи.

І-й етап – виявлення потреби для вдосконалення фінансової безпеки підприємства. Під час цього етапу можна провести «форензік аудит» та знайти, наприклад, «слабкі сторони».

ІІ-й етап – автоматизація бізнес процесів раціональне використання виробничих фондів шляхом застосування новітнього програмного забезпечення. В свою чергу автоматизацыя бызнес процесыв також можна поділити на кроки.

Крок перший – визначення цілей автоматизації.

Крок другий – формування списку вимог до рішення.

Крок третій – моніторинг ринку на предмет наявності інструментів, і провайдерів що впроваджують ці інструменти.

Крок четвертий – формування і узгодження орієнтовного бюджету проекту.

Крок п’ятий – впровадження обраних рішень.

Впровадження певних систем та розробок допоможе пришвидшити та покращити продажі, розрахунок фінансових показників, аналіз підприємства на багатьох рівнях. Наприклад CRM – системи допомагають вести облік та робити швидкий аналіз стану підприємства. Чат-бот для продажів – допоможе

підвищити продажі, за рахунок того, що людям зручніше замовити у декілька кліків.

III-й етап – впровадження технологій забезпечення фінансової безпеки підприємства. З підрозділу 3.1. можна зробити висновок, що потрібно зберігати дані не лише на сервірах але і у хмарі, для постійного доступу до послуг. Також впровадження вже розроблених сервісів для забезпечення безпеки від загроз – допоможе вдосконалити фінансову безпеку підприємства.

IV-й етап – навчання робітників. Після впровадження певних сервісів та систем, потрібно ознайомити працівників з новітніми технологіями. Це можна зробити в різних варіаціях:

– запрошення спеціаліста та проведення корпоративного навчання;
– проходження онлайн курсів;
– найм спеціаліста на посаду.

Схематично етапи впровадження виглядають (рис.3.5):

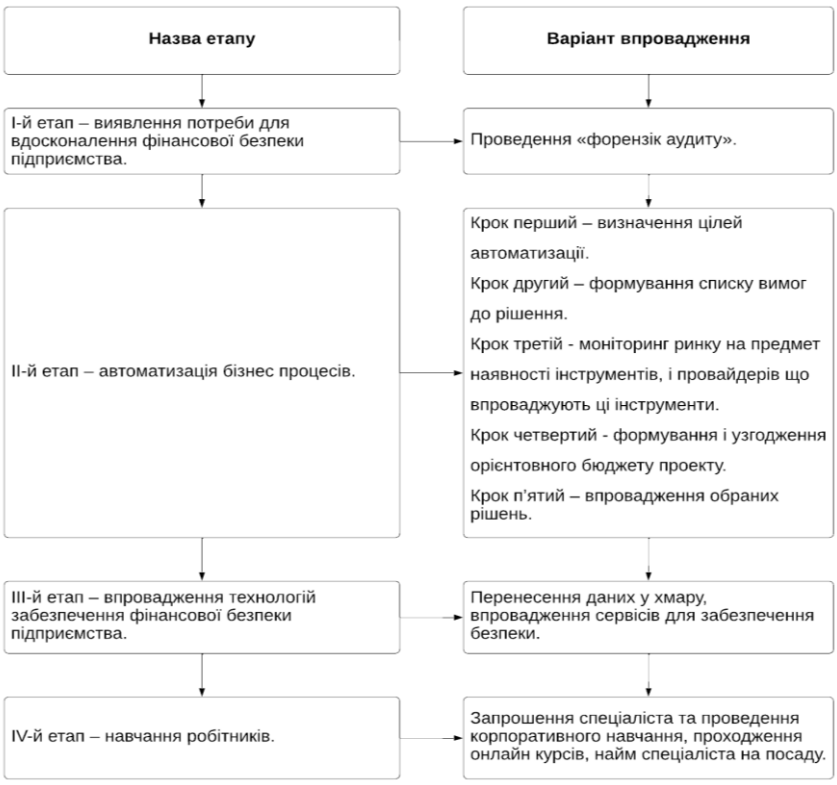


Рисунок 3.5 – Схема забезпечення фінансової безпеки підприємства з застосування технологій цифрової економіки

Наступною технологічною розробкою – є універсальний чат-бот, в якому зібрана інформація, корисні сервіси, поради, та посилання на готові таблиці для розрахунку фінансових показників підприємства.

Мета, завдання та етапи розробки чат-боту.

Мета: застосування технологій розробки чат-боту для підкреслення потреби впровадження їх у бізнес.

Завдання: створення «бібліотеки» інформації, яка можна завжди застосовувати. Основне меню чат-боту наведено на рис. 3.6, приклад роботи чат-боту на рис. 3.7.

Етапи розробки.

І-й етап: виявлення ідеї та теми на яку буде направлена розробка. В цьому чат-боті підкреслена ідея наявності бібліотеки сервісів які будуть у нагоді для бізнеса, google таблиць для розрахунку коефіцієнтів фінансової стійкості та інших фінансових розрахунків, огляд трендів та технологій які застосовуються у фінансової безпеці, та поради щодо покращення фінансової безпеки.

ІІ-й етап: пошук інформації.

На цьому етапі для кожної з кнопок: новітні тренди; поради щодо забезпечення фінансової безпеки підприємства; база посилань які будуть у нагоді для кожного підприємства (юридичні послуги, open data, аналіз конкурентів та ін.); сервіси які можна впровадити для забезпечення фінансової безпеки підприємства; посилання на Google-таблиці для фінансових розрахунків; буде додана інформація, яка вже висвітлена в цієї кваліфікаційної роботі, з якої зроблено висновок і поради, а також пошук сервісів які будуть у нагоді кожному підприємцю.

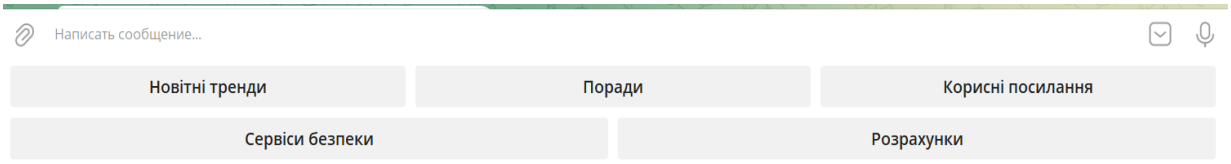


Рисунок 3.6 – Основне меню чат-боту

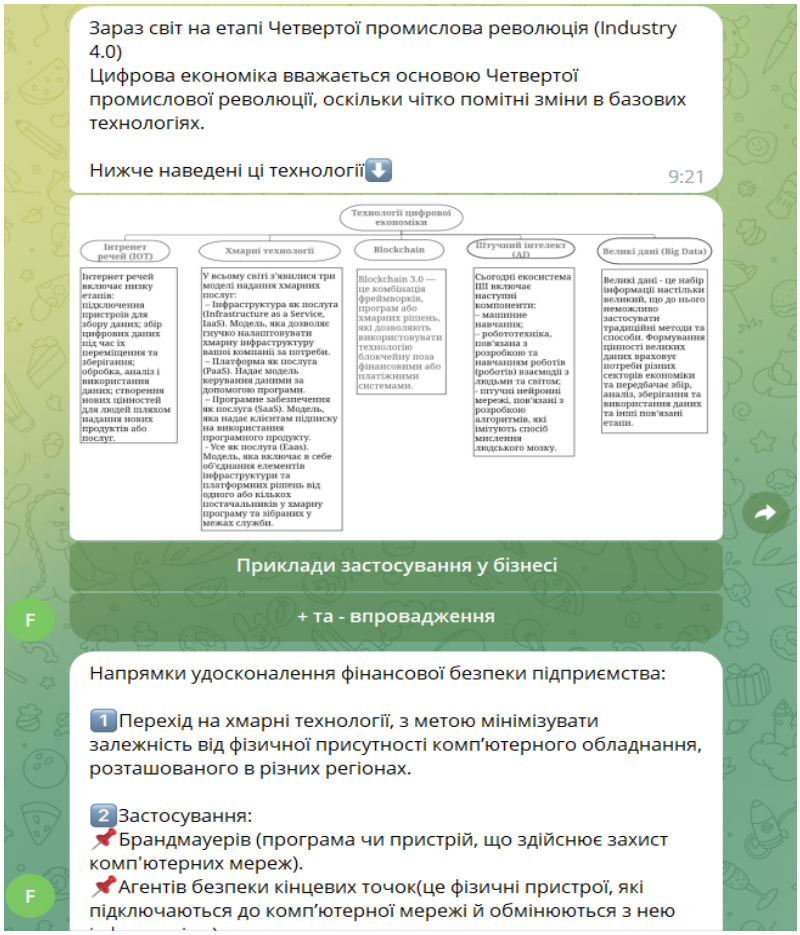
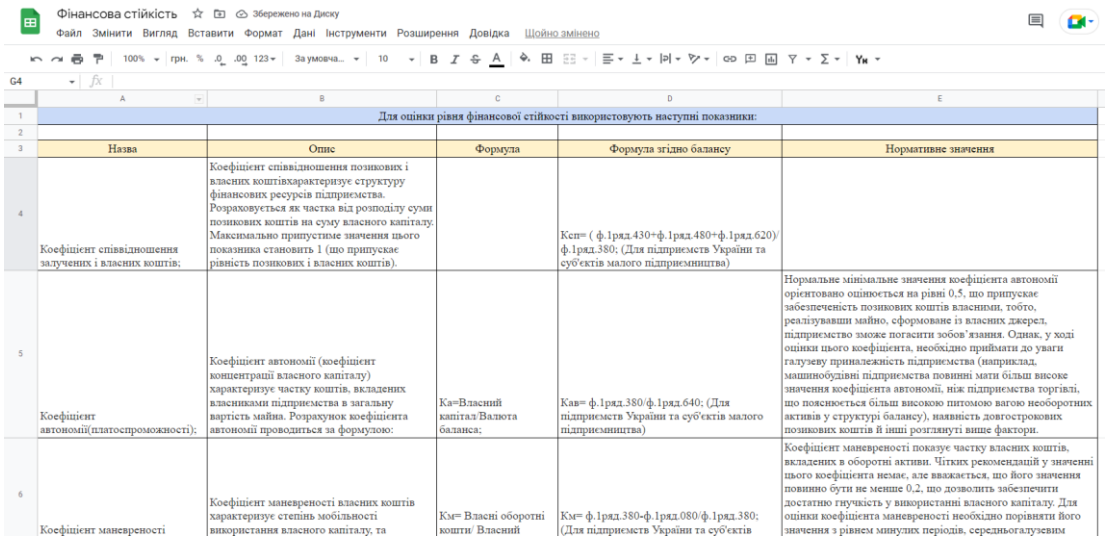


Рисунок 3.7 – Приклад роботи чат-боту

Наприклад, будуть додані посилання на такі сервіси як: доступ до державних даних для громадян та бізнесу, онлайн-сервіс перевірки компаній та ін.

ІІІ-й етап: створення Google таблиць для автоматизації розрахунків (рис.3.8).

Під час цього етапу розроблена Google таблиця розрахунку фінансової стійкості, а також надані посилання на шаблони Google таблиць, такі як: баланс, інвентаризація, CRM-система.



Фінансова стійкість

Збережено на Диску

Файл Змінити Вигляд Вставити Формат Дані Інструменти Розширення Довідка Щойно змінено

	A	B	C	D	E
1	Для оцінки рівня фінансової стійкості використовують наступні показники:				
2					
3	Назва	Опис	Формула	Формула згідно балансу	Нормативне значення
4	Коефіцієнт співвідношення залучених і власних коштів;	Коефіцієнт співвідношення позикових і власних коштівхарактеризує структуру фінансових ресурсів підприємства. Розраховується як частка від розподілу суми позикових коштів на суму власного капіталу. Максимально припустиме значення цього показника становить 1 (що припускає рівність позикових і власних коштів).		Ксп= (ф.1ряд.430+ф.1ряд.480+ф.1ряд.620)/ ф.1ряд.380; (Для підприємств України та суб'єктів малого підприємництва)	
5	Коефіцієнт автономії(платоспроможності);	Коефіцієнт автономії (коефіцієнт концентрації власного капіталу) характеризує частку коштів, вкладених власниками підприємства в загальну вартість майна. Розрахунок коефіцієнта автономії проводиться за формулою:	Ка=Власний капітал/Валюта баланса;	Кав= ф.1ряд.380/ф.1ряд.640; (Для підприємств України та суб'єктів малого підприємництва)	Нормальне мінімальне значення коефіцієнта автономії орієнтовано оцінюється на рівні 0,5, що припускає забезпеченість позикових коштів власними, тобто, реалізувавши майно, сформоване із власних джерел, підприємство зможе погасити зобов'язання. Однак, у ході оцінки цього коефіцієнта, необхідно приймати до уваги галузеву приналежність підприємства (наприклад, машинобудівні підприємства повинні мати більш високе значення коефіцієнта автономії, ніж підприємства торгівлі, що пояснюється більш високою питомою вагою необоротних активів у структурі балансу), наявність довгострокових позикових коштів й інші розглянуті вище фактори.
6	Коефіцієнт маневреності	Коефіцієнт маневреності власних коштів характеризує степінь мобільності використання власного капіталу, та	Км= Власні оборотні кошти/ Власний	Км= ф.1ряд.380-ф.1ряд.080/ф.1ряд.380; (Для підприємств України та суб'єктів	Коефіцієнт маневреності показує частку власних коштів, вкладених в оборотні активи. Чітких рекомендацій у значенні цього коефіцієнта немає, але вважається, що його значення повинно бути не менше 0,2, що дозволить забезпечити достатню гнучкість у використанні власного капіталу. Для оцінки коефіцієнта маневреності необхідно порівняти його значення з рівнем минулих періодів, середньогалузевим

Рисунок 3.8 – Розроблена Google-таблиця коефіцієнти фінансової стійкості

IV-й етап: побудова алгоритму (рис.3.9).

Спочатку алгоритм будувався на аркуші, розраховувалась послідовність дій.

V-й етап: розробка чат-боту через конструктор.

Розроблений на IV-тому етапі алгоритм, перенесений у конструктор чат-ботів Smart Sender.

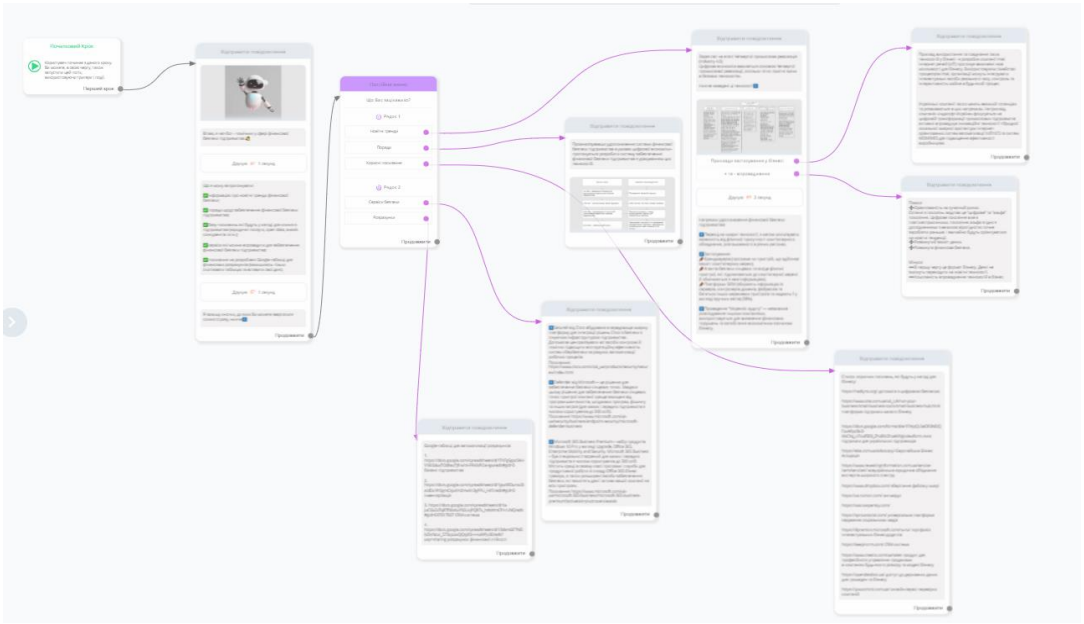


Рисунок 3.9 – Алгоритм чат-боту у конструкторі

VI-й етап: впровадження чат-боту.

Даний чат-бот може бути використаний кожним підприємцем, як база знань у сфері фінансової безпеки підприємства. Чат-бот є прикладом впровадження технологічної складової, яка логічно побудована і представляє доступ до неї цілодобово. Рекомендується впровадження такої технології для компанії «Cisco» з метою пояснення роботи продуктів безпеки, які вони презентують.

Посилання на розроблений бот: https://davidenko.customer. smartsender.eu/lp/EUxMIKbn.

Висновки до третього розділу

У третьому розділі проаналізовані напрямки удосконалення системи фінансової безпеки підприємства в умовах цифрової економіки, та визначені наступні тренди та технології:

- спеціальні програми які надають захист підприємства;
- технологія блокчейн захисту;
- форензік-аудит;
- технологія «Zero-trust».

Ринок з надання послуг захисту безпеки підприємств достатньо великий та постійно оновлюється.

Проаналізувавши в підрозділі 3.1 удосконалення системи фінансової безпеки підприємства в умовах цифрової економіки– пропонується розробити систему забезпечення фінансової безпеки підприємства з урахуванням цих технологій.

Для плавного переходу підприємства на більш якісне формування фінансової безпеки, пропонується впроваджувати поетапний підхід, який

поділяється на 4 етапи (виявлення потреби, автоматизація бізнес процесів, впровадження технологій, навчання робітників).

Наступною технологічною розробкою, яку проілюстровано в третьому розділі є універсальний чат-бот, в якому зібрана інформація, корисні сервіси, поради, та посилання на готові таблиці для розрахунку фінансових показників підприємства.

Даний чат-бот може бути використаний кожним підприємцем, як база знань у сфері фінансової безпеки підприємства. Чат-бот є прикладом впровадження технологічної складової, яка логічно побудована і представляє доступ до неї цілодобово. Рекомендується впровадження такої технології для компанії «Cisco» з метою пояснення роботи продуктів безпеки, які вони презентують.

ВИСНОВКИ

У цій кваліфікаційній роботі проявлено питання: «Як за допомогою нових технологій цифрової економіки забезпечити безпеку підприємства?». Переглянуті теоретичні засади безпеки підприємства та фінансового механізму. Ефективність фінансових механізмів є питанням забезпечення життєдіяльності будь-якого суб'єкта господарювання

Проведено оцінку діяльності компанії «Cisco» за допомогою аналізу фінансово-економічних показників за 2020-2022рр. Компанія забезпечила зростання загального доходу та високу прибутковість у складних умовах, на які вплинули значні обмеження поставок, зростання витрат на компоненти та пов’язаних із цим витрат. Як і раніше компанія зосереджена на впровадженні інновацій у технології, щоб допомагати клієнтам здійснити цифрову трансформацію. На компанію продовжують негативно впливати обмеження поставок, які спостерігаються в усій галузі через дефіцит компонентів. Компанія продовжує прогрес у перетворенні бізнес-моделі, надаючи більше програмного забезпечення та підписок.

Також переглянута стратегія забезпечення безпеки компанії «Cisco». Керівництво «Cisco» впровадило програму ERM, якою керує «Cisco», її функція – внутрішнього аудиту, щоб ідентифікувати, оцінювати ризики, контролювати та управляти ними. Структура програми ERM включає в себе як робочий комітет ERM, який фокусується на управлінні ризиками теми та виконавчий комітет ERM що складається з членів дирекції.

В цій кваліфікаційній роботі проведено аналіз сучасних технологій для забезпечення безпеки підприємства. Обґрунтовано та розроблено систему забезпечення безпеки підприємства.

Безперечною перевагою запропонованої системи є поетапний підхід, який дозволить спочатку проаналізувати стан підприємства, та

автоматизувати бізнес-процеси, потім за допомогою такої цифрової технології, як хмара – перевести дані в неї. Заключними етапами є впровадження спеціалізованих сервісів для забезпечення безпеки та навчання працівників. Ще однією технологічною розробкою є – чат-бот. Чат-бот був створений як «база знань» з безпеки для підприємств. У чат-боті використано теоретичні питання та відповіді яким присвячена ця робота, запропоновано розроблену в підпункті 3.1 – схему забезпечення безпеки, запропоновані Google-таблиці для розрахунків фінансових показників. Схожий бот, який буде направлений тільки на продукти компанії «Cisco» запропоновано впровадити як алгоритм прийняття рішень, щодо впровадження продуктів компанії у свій бізнес, але також цей бот може бути використаним кожним підприємцем.

Після реалізації запропонованої покрокової схеми забезпечення безпеки компанія «Cisco» може отримати такі переваги:

– для керівництва – можливість зберігати та утримувати базу початкових клієнтів, які ще не вирішили, яку розробку краще застосувати у своєму бізнесі;

– для клієнтів – розроблену покрокову модель дії з приводу забезпечення безпеки підприємства.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Артус М.М. Фінансовий механізм в умовах ринкової економіки. *Фінанси України*. 2005. № 5. С. 54-59.

2. Зятковський І.В. Теоретичні засади фінансів підприємств. *Фінанси України*. 2000. № 4. С. 17-26.

3. Берлач А. І. Безпека бізнесу: навч. посібник. Київ: Університет «Україна», 2007. 280 с.

4. Гонта О., Кальченко О. Фінансове планування на підприємствах реального сектору економіки. *Проблеми і перспективи економіки і управління.* 2017. № 4 (12). С. 128-133.

5. Барановський О. І. Філософія безпеки: Основи економічної і фінансової безпеки економічних агентів: монографія у 2 т. Т. 1. К.: УБС НБУ, 2014.. 831 с.

6. Нусінов В. Я., Астаф'єва К. О., Нусінова О. В. Оцінка рівня економічної безпеки підприємства на всіх етапах розвитку: монографія. ДВНЗ «Криворіз. нац. ун-т». Кривий Ріг: Чернявський Д.О., 2015. 185 с.

7. Рудніченко Є.М. Загроза ризик небезпека: сутність і взаємозв'зок системою економічної безпеки підприємства. *Економіка менеджмент підприємство*. 2013. №25 (І). С.188-195.

8. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки: навч. посібник. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

9. Іванченко Н., Кудрицька Ж., Рекачинська К. Бізнес-моделі в умовах цифрових трансформацій. URL: http://econ.Vernadsky journals.in.ua/journals/2020/31_70_3/31_70_3_2/33.pdf

10. Ляшенко В.І., Вишневський О.С. Цифрова модернізація економіки України як можливість проривного розвитку: монографія / НАН України, Ін-т економіки пром-сті. К.: 2018. 252 с.

11. Четверта промислова революція. URL: https://www.wiki.uk-ua.nina.az/Четверта_промислова_революція.html (дата звернення: 14.10.2022).

12. Апалькова В. В. Концепція розвитку цифрової економіки в Євросоюзі та перспективи України. *Вісник Дніпропетровського університету. Серія: Менеджмент інновацій*. 2015. Вип. 4. С. 9-18.

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

14. Мешко Н. П., Сазонець О. М., Джусов О. А., Пирог О. В., Сардак С.Е. Стратегії високотехнологічного розвитку в умовах глобалізації: національний та корпоративний аспекти: моногр. Дніпропетр. нац. ун-т ім. О. Гончара. Донецьк: Юго-Восток, 2012. 470 с.

15. Коровайченко Н. Ю. Передумови інтеграції України до єдиного цифрового ринку Європейського Союзу. *Ефективна економіка*. 2017. № 6. URL: http:// www.economy.nayka.com.ua/?op=1&z=5648.

16. Веретюк С. М., Пілінський В. В. Визначення пріоритетних напрямків розвитку цифрової економіки в Україні. *Наукові записки Українського науково-дослідного інституту зв'язку*. 2016. №2 (42). С. 51-58.

17. Kaikova, O., Terziyan, V., Tiihonen, T., Golovianko, M., Gryshko, S., & Titova, L. (2022). Hybrid Threats against Industry 4.0: Adversarial Training of Resilience. In *E3S Web of Conferences*. EDP Sciences.

18. «Цифрова адженда України – 2020 («Цифровий порядок денний – 2020)», ГС «ХАЙ-ТЕК ОФІС УКРАЇНА», 2016.

19. Artificial Intelligence Innovation Deloitte Report/ URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Artificial-Intelligence-Innovation-Report-2018-Deloitte.pdf 52.

20. Global Artificial Intelligence Industry Whitepaper. URL: https://www2.deloitte.com/cn/en/pages/technology-media-andtelecommunications/articles/global-ai-development-white-paper.html

21. Усенко А. Перспективы blockchain для бизнеса и украинской экономики. URL: https://home.kpmg.com/ua/ru/home/media/press-releases/2018/06/perspektivi-blockchain-dlya-biznesa-i-ukrainskoiekonomiki.html

22. Laney D. 3D Data Management: Controlling Data Volume, Velocity and Variety. META Group Research Note, 2001, No 6. URL: https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1611280

23. Макаров С.В. Соціально-економічні аспекти хмарних обчислень: монографія. К.: ЦЕМІ РАН, 2010. 216 с.

24. Butlin, J. (1989) “Our common future. by World Commission on Environment and Development. (London, Oxford University Press, 1987, pp.383.),” *Journal of International Development*, 1(2), pp. 284–287. Available at: https://doi.org/10.1002/jid.3380010208.

25. David, M. (2008) *Generation Z-striking the balance: Healthy doctors for a healthy community*. U.S. National Library of Medicine. Available at: https://pubmed.ncbi.nlm.nih.gov/18704218/ (Accessed: October 17, 2022).

26. Genevieve, B.S. (2020) *After Gen Z, meet Gen Alpha. What to know about the generation born 2010 to today*, *ABC News*. ABC News Network. Available at: https://abcnews.go.com/GMA/Family/gen-meet-gen-alpha-generation-born-2010-today/story?id=68971965 (Accessed: October 17, 2022).

27. Корольчук, М. (2019) Чим небезпечне кліпове мислення?, Learning.ua. Learning.ua. Available at: https://learning.ua/blog/201902/chym-nebezpechne-klipove-myslennia/ (Accessed: October 17, 2022).

28. Jacobson S. (2020) *Hype Cycle for Manufacturing Operations Strategy*. Available at: https://www.optessa.com/wp-content/uploads/2021/04/Gartner-Hype-Cycle-August-2020-with-Optessa.pdf (Accessed: October 17, 2022).

29. *Cisco*. URL: https://www.cisco.com/ (дата звернення: 17.11.2022).

30. Annual report reimagining the future of connectivity. 2022. URL: https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2022.pdf (дата звернення: 17.11.2022).

31. Remote Work: Keeping It Secure/ How Cisco scales our secure remote workforce. 2020. URL: https://www.cisco.com/c/dam/en_us/about/doing_business/trustcenter/docs/how-cisco-scales-our-secure-remote-workforce.pdf (дата звернення: 17.11.2022).

32. 2022 security visibility report [cisco]. 2022. URL: https://www.cybersecurity-insiders.com/portfolio/2022-security-visibility-report-cisco/ (date of access: 25.11.2022).

33. Фінансова безпека понад усе. ПриватБанк завершив міграцію у «хмару». ПриватБанк. URL: https://privatbank.ua/ru/news/2022/4/29/1637 (дата звернення: 25.11.2022).

34. Обсяги безготівкових розрахунків в Україні зростають, попри війну. Національний банк України. URL: https://bank.gov.ua/ua/news/all/obsyagi-bezgotivkovih-rozrahunkiv-v-ukrayini-zrostayut-popri-viynu (дата звернення: 25.11.2022).

35. Офіційний сайт Microsoft. URL: https://www.microsoft.com/uk-ua (дата звернення: 27.11.2022).

36. Офіційний сайт Oracle Corporation URL: https://www.oracle.com/ua/ (дата звернення: 27.11.2022).

37. Ющенко Н.Л. Блокчейн-технології в посиленні технологічного потенціалу України. *Стратегічні пріоритети соціально-економічного розвитку в умовах інституційних перетворень глобального середовища:*

матеріали VIII Міжнародної науково-практичної конференції (Одеса, 28–29 вересня 2018 р.). Одеса: ОНУ, 2018. С. 188–190.

38. Форензік – інструмент захисту Вашого бізнесу. Revealing Information - юридична компанія. URL: https://www. revealinginformation.com.ua/ (дата звернення: 27.11.2022).

39. What is zero trust security? Principles of the zero trust model. *Crowdstrike*. URL: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/ (date of access: 27.11.2022).

40. Першочергові сфери, ініціативи, проекти «цифровізації» України до 2020 року. *Цифрова адженда України – 2020 («Цифровий порядок денний» – 2020) Концептуальні засади*. 2016. URL: https://ucci.org.ua/ uploads/files/58e78ee3c3922.pdf (дата звернення: 17.11.2022).

41. Golovianko, M., Gryshko, S., Titova, L., & Filatov, V. (2022). *Good practices of Industry 4.0 in Ukraine.* URL:https://openarchive. nure.ua/handle/document/20985.

42. Четверта промислова революція: зміна напрямів міжнародних інвестиційних потоків / за наук. ред. д.е.н., проф. А.І. Крисоватого та д.е.н., проф. О.М. Сохацької. Тернопіль: Осадца Ю.В., 2018. 478 с.