МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТЕХНОЛОГІЙ

ННІ/факультет	Навчально-науковий інститут економіки та бізнес-освіти
Кафедра	міжнародних відносин
Спеціальність	292 Міжнародні економічні відносини
Форма навчання	денна

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

Котара Дениса Вікторовича
(прізвище, ім'я, по батькові здобувача)

на тему **Стратегії цифрового розвитку країн з урахуванням протидії кіберзагрозам**
(повна назва теми)

за матеріалами _____
(повна назва бази дослідження)

науковий керівник **к.е.н., доцент** _____ **Г. ПУРІЙ**
(наук. ступінь, вчене звання) *(підпис)* *(ініціал, прізвище)*

Робота допущена до захисту в ЕК
Протокол засідання кафедри
від «10» січня 2025 р. № 6
В.о. завідувача
кафедри _____
(підпис)
к.е.н., доцент І. ЄГОРОВА
Наук. ступінь, вчене звання *Ініціал, ПРІЗВИЩЕ*

Кривий Ріг – 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТЕХНОЛОГІЙ

ННІ/факультет	Навчально-науковий інститут економіки та бізнес-освіти
Кафедра	міжнародних відносин
Спеціальність	292 Міжнародні економічні відносини
Форма навчання	денна

«ЗАТВЕРДЖУЮ»
В.о. завідувача кафедри _____ І. ЄГОРОВА
(підпис) (Ініціал, ПРІЗВИЩЕ)
«20» січня 2025 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ МАГІСТЕРСЬКУ РОБОТУ
Котара Дениса Вікторовича

1. Тема роботи Стратегії цифрового розвитку країн з урахуванням протидії кіберзагрозам

Керівник роботи Пурій Ганна Володимирівна, к.е.н., доцент
затверджено наказом закладу вищої освіти від «25» жовтня 2024 р. № 733-ст

2. Строк подання здобувачем роботи до «22» січня 2025 р.

3. Зміст кваліфікаційної магістерської роботи, об’єкт, предмет та мета дослідження:

РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ МІЖНАРОДНИХ СТРАТЕГІЙ ЦИФРОВОГО РОЗВИТКУ КРАЇН
1.1 Теоретичний базис у сфері стратегій цифрового розвитку
1.2 Міжнародні бізнес-стратегії цифрової трансформації в умовах «Суспільства 5.0»
1.3 Міжнародний досвід реалізації програм та стратегії цифровізації
РОЗДІЛ 2 АНАЛІЗ ЦИФРОВОГО РОЗВИТКУ КРАЇН ТА СТРАТЕГІЙ ЇХ ЗАБЕЗПЕЧЕННЯ
2.1 Тенденції цифрової трансформації у світовій економіці
2.2 Цифровий ландшафт України
2.3 Аналіз впровадження та реалізації міжнародних стратегій кіберзахисту
РОЗДІЛ 3 ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ СТРАТЕГІЇ ЦИФРОВОГО РОЗВИТКУ УКРАЇНИ
3.1 Перспективні напрями реалізації стратегії цифрового розвитку України
3.2. Напрями удосконалення стратегії кібербезпеки України як гарантії національної безпеки

Об'єкт дослідження: процес дослідження перспектив стратегій цифрового розвитку країн з урахуванням протидії кіберзагрозам

Предмет дослідження: сукупність теоретичних, методологічних положень та інструментів дослідження стратегій цифрового розвитку країн з урахуванням протидії кіберзагрозам.

Мета кваліфікаційної магістерської роботи: теоретико - методологічне обґрунтування і розробка практичних рекомендацій щодо удосконалення стратегії цифрового розвитку країн з урахуванням протидії кіберзагрозам.

5. Дата видачі завдання «25» жовтня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної магістерської роботи	Строк виконання етапів роботи	Відмітка керівника про виконання етапів (дата, підпис)
1	Підготовка розділу 1	15.11.2024 р.	15.11.2024 р.
2	Підготовка розділу 2	10.12.2024 р.	10.12.2024 р.
3	Підготовка розділу 3	03.01.2025 р.	03.01.2025 р.
4	Перевірка кваліфікаційної магістерської роботи на наявність ознак академічного плагіату за допомогою програм UNICHECK / StrikePlagiarism	до 09.01.2025 р.	09.01.2025 р.
5	Отримання відгуку від наукового керівника	до 22.01.2025 р.	22.01.2025 р.
6	Подання кваліфікаційної роботи на перегляд завідувачу кафедри	до 22.01.2025 р.	22.01.2025 р.
7	Реєстрація завершеної кваліфікаційної роботи	22.01.2025 р.	Реєстраційний № 3 «22» січня 2025 р.
8	Попередній захист кваліфікаційної роботи на кафедрі	22.01.2025 р.	22.01.2025 р.
9	Підготовка до захисту в ЕК	до 24.01.2025 р.	до 24.01.2025 р.

Завдання підготував науковий керівник _____ Г. ПУРІЙ
(підпис) (прізвище та ініціали)

Завдання одержав _____ Д. КОТАР
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Котар Д. Стратегії цифрового розвитку країн з урахуванням протидії кіберзагрозам. - Рукопис.

Кваліфікаційна магістерська робота за спеціальністю 292 «Міжнародні економічні відносини» – Державний університет економіки і технологій. - Кривий Ріг, 2025.

111 стор., 6 табл., 20 рис., 2 додатки, 101 літературне джерело.

У дипломній магістерській роботі здійснено дослідження стратегій цифрового розвитку країн з урахуванням протидії кіберзагрозам.

Мета кваліфікаційної магістерської роботи – теоретико - методологічне обґрунтування і розробка практичних рекомендацій щодо удосконалення стратегії цифрового розвитку країн з урахуванням протидії кіберзагрозам.

Предметом дослідження є сукупність теоретичних, методологічних положень та інструментів дослідження стратегій цифрового розвитку країн з урахуванням протидії кіберзагрозам.

Об'єктом дослідження є процес дослідження перспектив стратегій цифрового розвитку країн з урахуванням протидії кіберзагрозам.

Досліджено теоретичний базис у сфері стратегій цифрового розвитку. Оцінено міжнародні бізнес-стратегії цифрової трансформації в умовах «Суспільства 5.0». Наведено міжнародний досвід реалізації програм та стратегії цифровізації.

Представлено тенденції цифрової трансформації у світовій економіці. Окреслено цифровий ландшафт України. Представлено аналіз впровадження та реалізації міжнародних стратегій кіберзахисту.

Окреслено перспективні напрями реалізації стратегії цифрового розвитку України. Представлено напрями удосконалення стратегії кібербезпеки України як гарантії національної безпеки.

Ключові слова: міжнародні стратегії, цифровізація, цифровий розвиток, кібербезпека, цифровий ландшафт, візія стратегії кібербезпеки.

ЗМІСТ

ВСТУП

Актуальність дослідження. Дедалі більша поширеність глобалізації та взаємопов'язаність міжнародних економічних, політичних і соціокультурних процесів зумовлює необхідність розробки та впровадження спільних стратегій для досягнення довгострокового розвитку на глобальному рівні.

Процес інтеграції цифрових технологій, автоматизації та ІТ у всі сфери життя та політики, а також економіки розпочався у другій половині 20-го століття і триває досі. Як правило, цей процес цифровізації є об'єктивним і спирається на глобальні процеси. Проте цей порядок, як і політичні та економічні відносини в цілому, відрізняється рядом ознак, недосконалостей і збоїв на ринку, які потребують державного контролю та регулювання.

Окрім добре відомих провалів ринку, таких як безробіття, монополізація, циклічність, соціальна нерівність, у цифровій економіці присутні специфічні провали ринку. Поряд з необхідністю економічного зростання вони є причиною виваженого підходу до державної політики та відіграють роль у цифровізації української політики. Як наслідок, створення та впровадження міжнародних стратегій розвитку має першочергове значення для досягнення довгострокового розвитку та покращення якості життя на Землі.

Ступінь розробленості проблеми, що досліджується. Чимало наукових досліджень присвячено теоретичним і практичним аспектам розробки та реалізації стратегій цифровізації в економічній сфері країн. До таких вітчизняних і зарубіжних вчених і фахівців належать: С.В. Войтко, Т.Є. Моісеєнко, Н.Є. Скоробогатова, К.М. Шваб, К. Скіннер та ін.

Значну увагу питанням цифровізації економіки та суспільства приділили вітчизняні та зарубіжні вчені, зокрема: В. Вишневський, О. Джусов, П. Друкер, С. Коляденко, І. Карчева, Б. Кінг, Ліпсі, Л. Лямін, В. Ляшенко, В. Пілінський, К. Скінер, Н. Стеблина, Е. Тоффлер, К. Шваб та ін. численні наукові дослідження, присвячені процесу оцифрування, вони все ще недостатні з точки зору дослідження.

Метою роботи є теоретико - методологічне обґрунтування і розробка практичних рекомендацій щодо обгрунтування міжнародних стратегій цифрового розвитку країн.

Завданнями роботи є:

- дослідити теоретичний базис у сфері стратегій цифрового розвитку;
- оцінити міжнародні бізнес-стратегії цифрової трансформації в умовах «Суспільства 5.0»;
- навести міжнародний досвід реалізації програм та стратегії цифровізації;
- представити тенденції цифрової трансформації у світовій економіці;
- окреслити цифровий ландшафт України;
- представити аналіз впровадження та реалізації міжнародних стратегій кіберзахисту;
- окреслити перспективні напрями реалізації стратегії цифрового розвитку України;
- представити візію стратегії кібербезпеки України як гарантії національної безпеки.

Предметом дослідження є сукупність теоретичних, методологічних положень та інструментів дослідження міжнародних стратегій цифрового розвитку країн.

Об’єктом дослідження є процес дослідження перспектив міжнародних стратегій цифрового розвитку країн.

Методи дослідження. Для вирішення поставлених завдань у роботі використовуються такі методи: пізнання; порівняльний; аналітичний; економічного аналізу (методи абсолютних, відносних та середніх величин, порівняння, групувань, індексний, балансовий, елімінування, прогнозування тощо); економіко-математичні («ex-post» прогнозування та кореляційний аналіз); евристичні (експертні) методи для формулювання мети, завдань роботи, висновків та рекомендацій щодо кількісних і якісних характеристик показників

міжнародних стратегій цифрового розвитку країн (індукції та дедукції, систематизації та узагальнення; логіко-формалізовані.

Використання зазначених методів забезпечує практичність, універсальність, реалістичність та достовірність отриманих результатів.

При написанні роботи використано сучасні інформаційні технології, математичні методи та ЕОМ, зокрема ППП «Excel», текстовий редактор Word, ресурси INTERNET тощо.

Інформаційною базою дослідження є законодавчі та нормативно-правові акти, Закони України, фахова література, матеріали наукових конференцій та періодичних видань; статистичні дані Всесвітніх організацій, Головного управління статистики України, інформаційні ресурси мережі Інтернет.

На захист роботи виносяться науково-дослідницькі положення щодо: перспективних напрямів реалізації стратегії цифрового розвитку України; візії стратегії кібербезпеки України як гарантії національної безпеки.

Практична цінність роботи: розроблені в ході дослідження підходи, теоретичні узагальнення, висновки та рекомендації можуть бути використані для вибору альтернатив міжнародних стратегій цифрового розвитку країн.

Обсяг та структура кваліфікаційної магістерської роботи. Основний зміст роботи викладено на 111 сторінках комп’ютерного тексту, включаючи вступ, три розділи, висновки, рекомендації. Список використаних джерел містить 101 джерело. У роботі наведено 6 таблиць, 20 рисунків, 2 додатки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ МІЖНАРОДНИХ СТРАТЕГІЙ ЦИФРОВОГО РОЗВИТКУ КРАЇН

1.1 Теоретичний базис у сфері стратегій цифрового розвитку

Концепція цифрового розвитку часто неправильно тлумачиться як пов’язана з цифровою трансформацією чи оцифруванням, але насправді вона відрізняється від цих інших концепцій. У той час як цифровий розвиток пов’язаний із забезпеченням доступу до цифрових технологій для всіх людей у суспільстві, цифрова трансформація поєднує цифрові технології з давно існуючими аналоговими технологіями для досягнення стану конвергенції та узгодженості. Цифрова трансформація бізнесу вимагає системного підходу або технологічної конвергенції, і комбінації цифрових технологій використовуються для зміни моделі бізнесу, продуктів, послуг, бачення та основних сфер бізнесу. З іншого боку, цифровий розвиток сприяє універсальному доступу до ІКТ, включаючи фізичні пристрої та комп’ютеризовані програми, для всіх осіб і домогосподарств у суспільстві. Термін «оцифрування» вперше був використаний у 1960-х роках, а термін «оцифрування» — у 90-х роках. Сьогодні слово «цифрування» є загальновживаним, тоді як «оцифрування» все ще широко використовується. Ці терміни є синонімами. Спільність між цифровою трансформацією та оцифруванням є в контексті Індустрії 4.0, однак остання більше стосується концепції оцифрування, оскільки вона стосується традиційної літератури.

Ресурсомісткий і складний характер цифрової трансформації в Індустрії 4.0 відрізняє її від цифровізації. Менші компанії повинні мати особливі здібності, наприклад, мати справу зі змінами та мати потенціал.

Стратегічний план цифровізації, спрямований на досягнення певного рівня інформаційної, цифрової, операційної та кіберрозвиненості, називається кіберпланом. Це пояснює різницю між цифровим розвитком і цифровою

трансформацією або оцифруванням, остання з яких передбачає інший набір можливостей і зосереджується на наданні доступу до технологій, а не на модифікації існуючих систем або процесів.

Цифрова революція має на меті використовувати технології для сприяння соціальному та економічному розвитку, насамперед у країнах, що розвиваються. Глобальний підхід Світового банку до цифрового розвитку полягає в партнерстві з урядами країн, що розвиваються, з метою створення основ для відповідального та інклюзивного цифрового розвитку. Це передбачає створення цифрової інфраструктури, вдосконалення цифрових знань і здібностей, а також забезпечення рівномірного розподілу переваг цифрових технологій між усіма членами суспільства. Загалом цифровізація є важливою складовою сьогоднішніх зусиль розвитку, ймовірно, її важливість з часом зростатиме, оскільки технології продовжуватимуть розвиватися.

Результати дослідження думок кількох експертів, сформованих ними на основі власного досвіду, свідчать про те, що цифровий розвиток вважається початком, використання цифрових технологій та цифрових інструментів у всіх сферах життя, це призводить до створення інноваційних продуктів, послуг і рішень, які позитивно впливають на ефективність, продуктивність і конкурентоспроможність у різних сферах. Це пов’язано з використанням комп’ютерів і цифрових інструментів для створення нових технологій, платформ і систем, які задовольняють запити користувачів і вирішують соціальні проблеми [12, с. 29].

Категоріальний апарат у сфері цифрової політики складається із лексики, яка визначає основні поняття та ідеї, пов’язані з розробкою та реалізацією державної політики у цій сфері.

Як зазначає Кожина А. «одним із першочергових напрямків державного управління в нинішньому стані справ і в масштабах країни є перехід до цифрової трансформації державного управління та розвиток цифрового суспільства» [19, с. 134].

Островій О. Політику держави щодо цифрового розвитку слід розглядати як систему тактики державного управління, що базується на чинних правових нормах, які узгоджені цілями, ці цілі покликані сприяти реалізації функцій держави щодо цифрової трансформації з мета підвищення поширеності цифрових технологій у всіх сферах суспільного життя та забезпечення належних умов і можливостей для цифровізації національної економіки.

Результати дослідження свідчать про те, що державна політика цифрового розвитку в ЄС має передусім стратегічний характер, що включає реалізацію «цифрового порядку денного» на національному та наднаціональному рівнях з метою каталізації цифрової трансформації та створення Єдиного цифрового ринку ЄС.

Важливо підкреслити, що відмінними рисами цифрового розвитку згідно з українським законодавством є «прискорення економічного зростання та підвищення залучення інвестицій; перетворення секторів економіки на більш конкурентоспроможні та ефективні; технологічна та цифрова модернізація галузей, створення високотехнологічних виробництв. ." [24]. Тобто цифрова еволюція є ознакою впровадження цифрових технологій у суспільство, це безпосередньо впливає на економічне зростання та розвиток різних сфер життя [27, с. 149].

В ідеї розвитку цифрової економіки та суспільства України на 2018-2020 роки зазначено, що «цифровий розвиток передбачає реалізацію низки дій, які позитивно вплинуть на економіку, бізнес, суспільство та умови життя країни в цілому». [25].

Основоположні принципи політики цифрового розвитку держави закріплені численними нормативно-правовими актами України, метою яких є сприяння розвитку цифрової інфраструктури країни. Постанова Кабінету Міністрів «Деякі питання цифрового розвитку» описує принципи державної політики щодо цифрового розвитку, яка включає зобов’язання щодо цифрових перетворень України [18].

Проте, як країна, яка має намір стати членом ЄС, ми також повинні обговорювати та впроваджувати європейський досвід у впровадженні та розширенні цифрової стратегії держави для просування до єдиного цифрового ринку ЄС. Основними європейськими напрямками цифрового розвитку, як визначено Ініціативою EU4, є [28, с. 6]:

- нормативні акти щодо телекомунікацій;

– довіра та безпека;

– цифрова торгівля;

- досягнення ІКТ;

- електронна система охорони здоров'я;

- цифрові здібності.

Враховуючи вищезазначене, методи реалізації політики цифрового розвитку держави є надзвичайно важливими для розвитку цифрової економіки та конкурентоспроможності держави у світовому співтоваристві. Спільною рисою цифрового розвитку в розвинутих країнах є міжнародна співпраця та інтеграція, що виражається у створенні стандартів, протоколів та інтерфейсів, які покликані забезпечити сумісність. Крім того, багато зусиль докладається для створення правової системи [22, с. 87].

Значення цифрового розвитку та його наслідки описав у своїй дисертації, представленій у 2009 році, вчений Ісмаель Пенья-Лопес під керівництвом Тіма Келлі. Їхні дослідження показали, що державна політика, яка сприяє розвитку інформаційного суспільства (тепер це цифрове суспільство та метавсесвіт), дійсно важлива з кількох причин: вихідні точки; мультиплікаційний ефект; час; кадрів [14, с. 13].

Науковець Ісмаель Пенья-Лопес у своєму дослідженні визначає, що державна політика цифрового розвитку необхідна насамперед для подолання цифрового розриву в країнах, які йдуть на цифровий розвиток.

Цифровий розрив характеризується нерівним доступом до інформаційних технологій і методів комунікації між різними соціальними групами та регіонами.

Це може включати доступ до Інтернету, комп'ютерів, мобільних телефонів та інших технологій, пов'язаних із цифровим зв'язком [14].

У статті «подолання цифрового розриву в Україні: підхід, орієнтований на людину» з сайту ПРООН розглядається питання цифрового розриву в Україні. Розслідування показало, що цифровий розрив є особливо проблематичним для осіб з низьким рівнем доходу, людей похилого віку, жінок і тих, хто живе в сільській місцевості. Це приклад впливу цифрового розриву на окремі громади. Тому вкрай важливо враховувати це питання при розробці політики цифрового розвитку держави.

У результаті можна зробити висновок, що механізми реалізації державної політики щодо цифрового розвитку є вирішальними для успішної реалізації цілей і завдань держави в цифровій сфері. Розглянувши всі вищезазначені терміни, вважаємо, що найефективніше буде визначити поняття «механізм реалізації політики цифрового розвитку держави» в контексті українських реалій, як сукупність методів і процедур, що сприяють ефективній реалізації державної політики у сфері цифрового розвитку. Ці інструменти можуть включати фінансові винагороди, закони, програмні продукти та послуги, а також спеціалізовані організації, які наглядають за виконанням політики. Механізми реалізації політики цифрового розвитку держави сприяють забезпеченню стабільності та сприяють розвитку у цій сфері, що сприяє досягненню стратегічних цілей і завдань держави.

Як результат, стратегії цифрового розвитку країн включають низку дій, спрямованих на забезпечення швидкого та ефективного поширення цифрових технологій у всіх сферах суспільства. Ось деякі з найважливіших стратегій:

1. Комунікаційна інфраструктура: створення швидкого підключення до Інтернету (включаючи мережі 5G) і розширення мобільного зв'язку для покриття всієї країни, щоб кожен міг отримати доступ до Інтернету.

2. Цифрова освіта та навчання: Створення програм, які сприяють розвитку цифрових здібностей серед населення та бізнес-спільноти. Це можна реалізувати

як через освіту з програмування, так і через інформаційні технології та цифрову грамотність.

3. Цифрове державне управління: впровадження електронного уряду та електронних послуг для громадян і бізнесу. Це може включати електронне голосування, електронну охорону здоров'я та освіту, а також електронне оподаткування та фінансове управління.

4. Інноваційна екосистема: Створення відповідного середовища для зростання та інтеграції інноваційних технологій. Це може включати підтримку нових компаній, створення інкубаторів і технопарків, сприяння науковим дослідженням і залучення іноземних грошей.

5. Кібербезпека: розробка стратегій і планів кібербезпеки для захисту критичної інфраструктури, освітніх та інституційних систем від кібернападів.

6. Розвиток цифрової економіки: з огляду на розвиток цифрових технологій у виробництві, сільському господарстві та інших сферах, це призведе до підвищення продуктивності та економічної конкурентоспроможності.

7. Доступність даних та інновації: надання громадськості доступу до відкритих даних та сприяння інноваціям у суспільстві та бізнесі.

Ці стратегії мають на меті створити цифрове суспільство, яке є більш ефективним, дієвим і сталим у світовій спільноті.

1.2 Міжнародні стратегії цифрової трансформації в контексті «Суспільство 5.0»

Нещодавно з появою нового покоління цифрових технологій відбулися значні зміни в бізнесі та соціальній сфері, які вважаються «наскрізними» через їх масштаб і глибину впливу. Цифрова трансформація бізнес-процесів є надзвичайно важливою темою в сучасному світі, оскільки технологічний розвиток, конкуренція та мінливі умови вимагають постійної уваги до нових ситуацій. Саме використання цифрових технологій сприяє створенню ефективних стратегій, знижує витрати, підвищує ефективність і якість роботи,

забезпечує швидкість і точність прийняття рішень, покращує комунікацію зі споживачами та партнерами, а також розробляє нові продукти та послуги.

Дослідження питань, пов'язаних із міжнародними бізнес-стратегіями щодо цифрової трансформації в контексті «Суспільства 5.0», має важливе значення для досягнення успіху в сучасному світі, це дозволяє людям бути конкурентоспроможними, ефективними та інноваційними.

У наукових публікаціях полеміку навколо цифрової трансформації бізнес-процесів та її вплив на бізнес та всю економіку обговорювали Н. М. Краус, Н. М. Краус, О.І.Н. Марченко, О. Ф. Новікова, Г. М. Дергачова, Я.А.Т. Колешній, А. Аєта, К. Шукець, М. Є. Дойч, О.І.Н. Панкова Н. І. Н. Рагуліна, Ю.В. Кіндзерський, В. Т. Тахтаров, П. Л. Гринько та ін. [27-42]. У багатьох наукових дослідженнях у цій сфері розглядалися різні аспекти впливу цифрової трансформації, особливості створення бізнес-процесів у цифровому середовищі та особливості впливу цифровізації на національну економіку. У творчості Н.М.Тягунової, З.А.Т. Тягунова, К. М. Молчанова та ін. [43, 44] досліджували вплив цифрової трансформації на клієнтський досвід і зміни споживчого попиту та поведінки, вони також охарактеризували вплив цифрової трансформації на конкурентний ландшафт та інноваційний характер компаній.

Міжнародні стратегії бізнесу досліджують М. Портер (його ідеї, такі як «ланцюжок вартості» та «стратегічні групи», стали основою для розробки міжнародних стратегій), І. Ансофф (досліджував концепцію ринкового вторгнення, зростання ринку, розвиток продукту та спеціалізація як стратегічний підхід для міжнародних корпорацій), Х. Хемел наголошував на інноваціях та створенні унікальних переваг у конкуренції). Проте дослідження специфіки становлення «суспільства 5.0» та впливу цифровізації на створення бізнес-стратегій на міжнародних прикладах є необхідним для адекватного пояснення цього явища [28].

Дослідження властивостей цифрової трансформації стратегій міжнародного бізнесу в контексті становлення «Суспільства 5.0» має важливе значення для підприємств та економіки в цілому. Це полегшує розуміння впливу

цифрових технологій і нових інновацій на стратегічне управління та конкурентоспроможність міжнародних компаній.

Як правило, міжнародні бізнес-стратегії підприємства є складною концепцією, що розвивається, тому їх потрібно постійно оцінювати та модифікувати у відповідь на зміни зовнішнього середовища на міжнародній арені. Ефективна реалізація та розробка цих стратегій є вигідною для компаній, оскільки вона дає їм міцну позицію на світовому ринку та сприяє довгостроковому розвитку.

Конверсія бізнес-стратегій - це, перш за все, зміна традиційних методів і підходів, які використовуються для виконання різних функцій і операцій в компанії. Це досягається завдяки використанню сучасних технологій та інновацій. Метою цієї трансформації є підвищення ефективності та продуктивності бізнес-процесів, зниження витрат, підвищення якості продукту чи послуги та підвищення рівня задоволеності клієнтів.

Зміна бізнес-стратегії також призводить до зміни способу проведення бізнес-процесів, що може бути викликано зміною бізнес-моделі компанії та/або вимог клієнтів, екологічних норм або просто впровадженням нових технологій у ділова сфера. Одним із компонентів трансформації бізнес-процесів є культурна зміна в організації, яка представлена зміною підходу до праці та переходом до нових ідей. Сьогодні цій трансформації сприяє процес цифровізації, створення нової реальності – «Суспільство 5.0» [28]. Характеристика цифрової трансформації бізнес-процесів на підприємствах, що входять до «Суспільства 5.0», включає наступні складові (рис.1.1).

Використання розумних технологій: це включає використання штучного інтелекту, аналізу даних, Інтернету речей (IoT), роботів, блокчейну та інших розумних технологій, призначених для оптимізації бізнес-процесів.

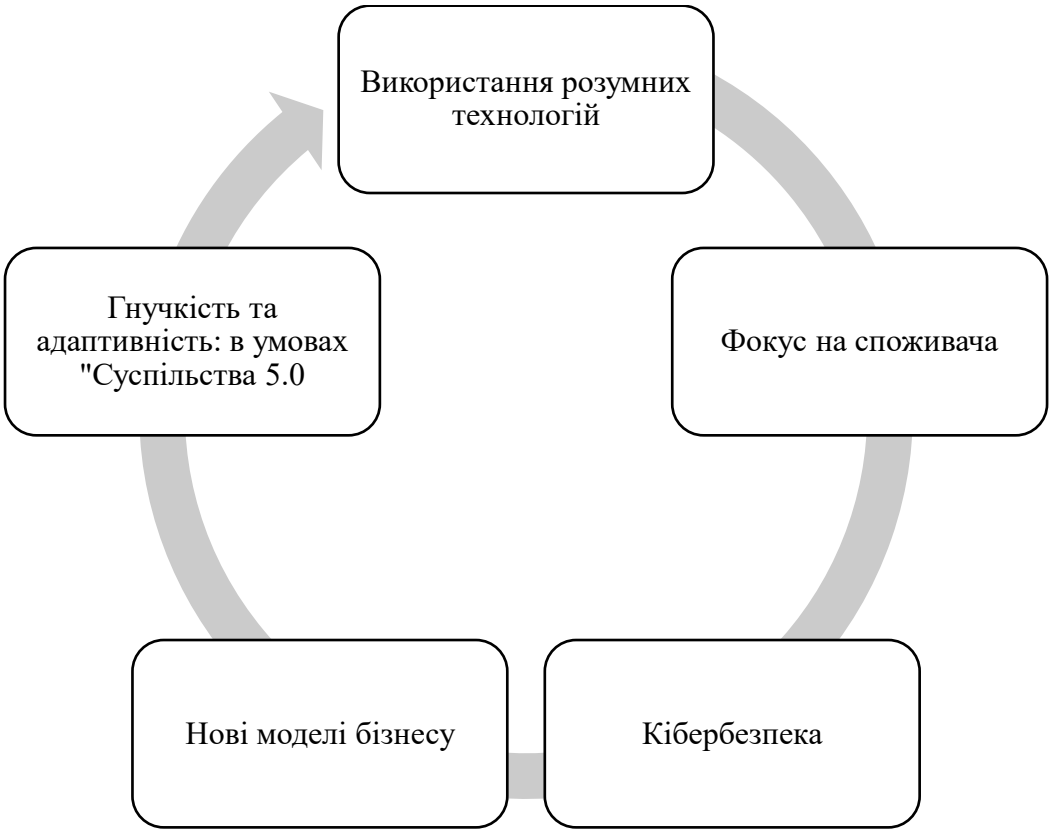


Рис.1.1. Складові цифрової трансформації бізнес-процесів у контексті «Суспільство 5.0»

Примітка. Джерело: побудовано авторами за [29]

Увага до споживача: цифрова трансформація спрямована на покращення споживчого досвіду, забезпечення підвищення якості продуктів і послуг, а також підвищення рівня задоволеності продуктом.

Нові бізнес-моделі: це включає створення нових бізнес-моделей на основі використання інтелектуальних технологій, наприклад, платформ спільного використання ресурсів, екологічних бізнес-моделей тощо.

Гнучкість і адаптація: в контексті «Суспільства 5.0» компанії повинні бути готові до змін і вміти швидко та ефективно пристосовуватися до нових умов ринку та нових викликів.

Кібербезпека: збільшення кількості кібератак і злочинів проти комп’ютерів у зв’язку з цифровою трансформацією бізнесу вимагає додаткових заходів для забезпечення кібербезпеки.

Бізнес-ландшафт також розвивається завдяки цифровим технологіям, продуктам, інструментам і послугам, які зараз вважаються найважливішими для сучасного соціального та економічного середовища. Цифровізація суттєво впливає на наше мислення, нашу мотивацію до прийняття рішень, а також на економічну поведінку підприємств, організацій, принципи бізнесу та економіки в цілому.

Багато провідних країн беруть участь у цифрових стратегіях у міжнародному бізнесі, застосовуючи різні дії та підходи. Сьогодні Китай, Сінгапур, Швеція, Естонія та Японія визнані провідними країнами у впровадженні цифрових стратегій. Наприклад, у Сінгапурі застосована стратегія «Сінгапур у режимі цифрової економіки», яка стосується використання технологій для розвитку фінансової, медичної, транспортної, освітньої та інших галузей. У Швеції, окрім активного просування цифрових технологій у різних сферах, цікавить також концепція «цифрового громадянства», яка спрямована на сприяння цифровій безпеці. Сьогодні Китай, як правило, вважається провідною країною в області цифрових технологій, особливо в сфері електронної комерції та мобільних платежів. Китай сприяє використанню штучного інтелекту, великих даних та інших передових технологій для розробки інноваційних рішень у сферах транспорту, охорони здоров’я, енергетики тощо.

У результаті можна визначити компоненти, які конкретно залучені до просування цифрових стратегій (рис. 1.2).

Країною, яка найбільш успішно реалізує стратегію «Суспільство 5.0», є Японія, яка вперше запропонувала концепцію «Суспільство 5.0» у 2016 році. Під час реалізації цієї концепції Японія має численні труднощі, які перешкоджають сталому розвитку її економіки та мають негативний вплив на соціальну сферу. Серед проблем можна назвати зменшення робочої сили, старіння населення, екологічні проблеми, обмеженість базових ресурсів тощо. Якщо ці проблеми не вирішити, Японія може стати менш конкурентоспроможною. Щоб уникнути цього сценарію, японська бізнес-спільнота «Кейданрен» виступила з ініціативою створення цілісної концепції «Суспільство 5.0». Ця ідея була спрямована на

вирішення значних проблем у країні та передбачала розробку нових рішень існуючих проблем та використання цифрових технологій для покращення життя громадян та сприяння динамічному розвитку країни [32].

Рис.1.2. Заходи, спрямовані на розвиток цифрових стратегій на національному рівні

Примітка. Джерело: побудовано авторами за [30, 31]

Тобто Японія дотримується стратегії «Суспільство 5.0» як основи розробки та впровадження інноваційних рішень, які матимуть значний вплив на розвиток суспільства та економіки та забезпечуватимуть постійну конкурентоспроможність країни в глобальному контексті.

Розробляючи цю концепцію, уряд Японії виходив з основних проблем, які перешкоджають сталому розвитку японської економіки та світової спільноти, а також негативних соціальних наслідків: зменшення чисельності населення та старіння робочої сили, посилення міжнародної конкуренції, необхідність оновлення інфраструктури, стихійні лиха та тероризм, екологічні проблеми та брак ресурсів.

Загалом концепція «Суспільство 5.0» – це опис суспільства майбутнього, яке випливає із взаємодії трьох компонентів: людини, технологій і природи. У цьому суспільстві очікується розвиток різноманітних інноваційних технологій, які мають на меті покращити якість життя людей і зменшити вплив людини на світ природи.

На нашу думку, найважливішими пріоритетами «Суспільства 5.0» є: розвиток економіки на основі технологічних інновацій, використання штучного інтелекту, роботів та Інтернету речей для покращення якості життя людей та оптимізації процесів. у різних сферах життя, включаючи сільське господарство, транспорт, охорону здоров я, освіту та інфраструктуру, створення відкритої науки та освіти, а також підвищення рівня соціального забезпечення. Насправді «Суспільство 5.0» — це майбутнє, до якого ми готуємося вже сьогодні, використовуючи сучасні технології та наукові досягнення.

У деяких аспектах концепція «Суспільство 5.0» походить від концепції «Індустрії 4.0», яка була популяризована Німеччиною та подібними ініціативами в інших країнах. Ці країни прагнуть здійснити четверту (інформаційну) промислову революцію.

Однак концепція Японії є більш широкою, вона намагається модернізувати суспільство та економіку через посилення формування капіталу. Суспільство 5.0 відкриває нову еру економічного та соціального прогресу, яка

долає дефіцит інформації та нерівність між науковцями та виробниками технологій у рамках Індустрії 4.0 та забезпечує гармонійний розвиток науки та технологій з урахуванням інтересів усіх членів суспільства.

У результаті в «Суспільстві 5.0» нестачу робочої сили можна компенсувати за рахунок використання переваг нових технологій для допомоги літнім людям. Наприклад, роботів можна використовувати для підйому важких предметів, а пристрої, що покращують зір і слух, можуть збільшити можливості працевлаштування цієї демографічної групи. Ці рішення сприяють інклюзивному зростанню, покращують якість життя та залучають різні соціальні групи до економічного процесу.

Ці наміри в «Суспільстві 5.0» демонструють прагнення країни бути лідером у створенні більш співчутливого та стійкого суспільства, в якому технології використовуються для підвищення якості життя кожної людини та надання рівних можливостей усім. У «Суспільстві 5.0» бізнес-стратегії базуються виключно на використанні передових технологій і наукових інновацій для вирішення соціальних проблем і сприяння сталому зростанню. На нашу думку, важливо виділити наступні аспекти, що описують функціонування бізнес-стратегій у контексті «Суспільства 5.0»: орієнтація на людину (основна мета – задоволення потреб та підвищення якості життя людини); використання передових технологій, співробітництво та партнерство між різними суб’єктами, такими як компанії, державні органи, наукові установи та громадські організації; сталість та екологізація; і глобалізація ринків. Саме ці компоненти сприяють тому, щоб «Суспільство 5.0» стало каталізатором соціального прогресу, стійкості та економічного зростання.

Клієнт є центром розвитку сучасних корпорацій. Насправді компанії перейшли від традиційної маркетингової стратегії 4P (продукт, місце, ціна, просування) до більш сучасної стратегії 4C (узгодженість, вміст, зручність, контекст), яка орієнтована на клієнта, і стали прихильниками C- Концепція клієнта. Віра клієнта в продукт або послугу і його лояльність до них визначають його вибір продукту або послуги. Тобто замість традиційного підходу, який

зосереджувався на самому продукті, сучасні компанії фокусуються на потребах і вимогах клієнта. формування звички, створення мирного середовища, ставлення з повагою, передбачення проблем і потреб і створення сприятливого середовища для утримання клієнтів, яке не тільки сприяє лояльності, але й створює комфорт. Як описано вище, функція партнерства була значно посилена. Проте роль управління процесами значно зросла, тепер знання є основною формою переваги компаній на сучасному ринку. Очевидно, що незважаючи на вищезазначені тенденції значних економічних змін, метою компаній є підвищення власної вартості, підвищення привабливості інвестицій, збільшення зростання та розширення бізнесу.

Успішна цифрова стратегія служить орієнтиром для лідерів компаній і дозволяє їм впроваджувати цифрові ініціативи, оцінювати їх результати та розширювати свій бізнес, коли це необхідно. Однак на початку реалізації цифрової стратегії керівництво має обрати базову цифрову модель, яка буде реалізована: стратегія залучення клієнтів або стратегія цифрових рішень. Не розуміючи повного масштабу цифрової трансформації, менеджери не можуть створити стратегію, яка використовує переваги цифрових технологій у своєму бізнесі. Таким чином, він може не помітити майбутню загрозу до того, як настане час відповісти.

Необхідність цифровізації бізнесу буде тільки зростати. Навіть великі компанії, які традиційно були «аналоговими», зараз переходять на цифрові технології, створюючи продукти та формуючи окремі відділи інформаційних технологій. Крім того, «спадок Covid», конфлікт із Росією, продовжуватиме переслідувати нас вічно — те, як ми використовували свій офіс, більше не матиме значення. Багато компаній працюватимуть за гібридною моделлю, яка є професійною та прийнятною для компаній. У процесі розробки цифрової стратегії важливо зазначити, що цифровізація знищує економічну вигоду.

Цифровізація може навіть підірвати найефективніші стратегії додаткового доходу, що призводить до більшої цінності для споживачів, ніж для бізнесу. Ці деталі важливі для компаній і галузей, які хочуть перетворити

цифрові активи на грошову вигоду. Натомість вони мають ситуацію, коли перетворення прибуткового продукту чи послуги на його складові частини не залишає споживачам нічого для покупки, крім того, що їм потрібно. Оцифровка також призводить до того, що схеми розповсюдження стають неактуальними, надаючи різноманітні варіанти та прозорість цін. Будь-яку цифрову пропозицію, яку можна відтворити з обмеженими витратами та зусиллями, можна вважати віртуальною. У майбутньому впровадження цифрових технологій призведе до створення нових бізнес-систем і стратегій з відповідним вектором економічного зростання.

1.3 Міжнародний досвід реалізації програм та стратегії цифровізації

У більшості сучасних країн впровадження інформаційних технологій (ІТ) та розвиток складових цифрового суспільства вважаються одними з найважливіших стратегічних завдань і національних пріоритетів. Використання цифрових технологій, а також пов’язана з ними діяльність людини формує цифрову сферу сучасного суспільства. Ця сфера на сьогодні є важливою для економіки та інноваційного потенціалу держави, рівня освіченості та розвитку, ефективності державного управління та реалізації демократичних процесів.

Еволюція цифрових принципів зумовлює зростання вдосконалення методів і способів взаємодії в контексті економічних відносин. Використання інформаційних технологій сприяє збільшенню комунікаційних процесів, змінює склад і статус їх учасників, посилює децентралізацію управління державним і приватним секторами.

Як наслідок, у світі створилася нова реальність, яка вимагає впровадження політики цифрової економіки в масштабах усієї країни. Це досягається шляхом удосконалення відповідних законів системи, розробки масштабних стратегій, проектів і програм, зокрема, повного переведення сфери державного управління на цифрові технології.

Порівняння різних моделей розвитку цифрового суспільства, що мали місце у світі на той час, виявляє суттєву різницю в концептуальних підходах, пріоритетах, механізмах і методах реалізації. Проте ефективність їх застосування в першу чергу залежить від культурно-цивілізаційного складу країни, в якій вони реалізуються, внаслідок чого не існує універсальних моделей державного управління з використанням механізмів цифрової трансформації, механізму розвитку інституційного середовища країни. є першорядним [36].

Протягом останніх кількох років в Україні на національному рівні були розпочаті ініціативи щодо впровадження цифрових технологій у всі сфери суспільного життя з метою підвищення ефективності та зменшення витрат. Починаючи зі Стратегії сталого розвитку «Україна – 2020» [37], ця стратегія включала інші ініціативи та державні програми розвитку, які визначали Програму електронного урядування. У результаті держава зробила низку відповідних кроків, у тому числі створення концепцій, планів, стратегій, законів та інших формальних домовленостей.

Сьогодні політико-правовий клімат характеризується впровадженням цифрових технологій у контексті цифрової трансформації. З організаційної точки зору цьому процесу сприяє створення Комітету з питань цифрової трансформації у Верховній Раді України та Міністерства цифрової трансформації на національному рівні. Останнє було ініційовано урядом шляхом реформування Державного агентства з питань електронного урядування, яке передбачало трансформацію.

Цифровізація політики є результатом глобалізації та характеризується тим, що вона змінює поточні тенденції політичних процесів, мету політичних інститутів, соціальні взаємодії та потенційні сценарії майбутнього.

Цифровізація технологій визначає результати виборів, впливає на форму громадянської активності та впливає на зовнішню репутацію держави, вона також функціонує як каталізатор гібридності політичних систем, ідентифікує та легітимізує важливі фігури, кампанії та рішень.

Перехід на цифрові технології в політиці став все більш поширеним явищем у пострадянських країнах. Необхідність систематизації світового досвіду та пострадянського методу політичної цифровізації дозволяє зрозуміти призначення нового політичного актора/цифрового політичного суб'єкта, який змінює процеси підготовки до прийняття та реалізації політичних рішень, які на основі формування смислів у цифровому середовищі.

У вересні 2017 року Кабінет Міністрів України схвалив Концепцію розвитку електронного урядування в Україні [38], яка визначила електронне урядування як форму державного управління, яка сприяє ефективності, відкритості та прозорості діяльності органів державної влади. та органи місцевого самоврядування. Інформаційні та телекомунікаційні технології були використані для створення нової форми правління, яка орієнтована на потреби громадян. Впровадження системи електронного урядування базувалося на таких принципах: цифровий за замовчуванням; одноразове введення інформації; сумісність за замовчуванням; доступність та участь громадян; відкритість та прозорість інформації; довіра та безпека інформації. Досягнення мети Концепції досягнуто шляхом впровадження комплексних заходів у цих сферах: модернізації державних послуг та розвитку взаємодії між владою, громадянами та бізнесом через інформаційно-комунікаційні технології. Важливо зазначити, що ця ідея відрізняється від інших документів, які мають подібний зміст і складніший характер.

Для його реалізації застосовано План дій щодо реалізації Концепції розвитку електронного урядування в Україні [39], цей документ визначив обов'язки різних відомств і відомств та передбачив умови та методи контролю за їх виконанням.

У листопаді 2017 року КМУ затвердив Концепцію розвитку електронної демократії в Україні та план заходів щодо її реалізації [40], визначення електронної демократії полягає в тому, що це форма суспільних відносин, у яких беруть участь громадяни та організації. державотворення та в управлінні

державою, а також у місцевому самоврядуванні шляхом використання інформаційних технологій у демократичному процесі.

Реалізація концепції розрахована на два етапи, які триватимуть до 2020 року. Серед ініціатив електронної демократії однією із запропонованих процедур було вдосконалення способу подання та розгляду електронних петицій. План заходів щодо реалізації Концепції розвитку демократії в Україні містить завдання щодо нормативно-правового забезпечення та ресурсного забезпечення розвитку демократії в Україні, які виконуються державними інституціями за участю численних громадських організацій.

Перетворення політики в цифровий формат дозволяє новим політичним учасникам стати центром прийняття рішень через агрегацію численних мереж підтримки, це також створює загрозу для держав, які не мають необхідних інструментів для протидії наявній асиметричній інформації.

Перетворення політики в цифрове середовище має свої унікальні атрибути для кожної окремої держави, кожного політичного режиму та кожного окремого проекту. Гібридність сучасних політичних систем призводить до того, що процес цифровізації політики є більш розділеним, як наслідок, деякі показники свідчать про те, що авторитарні політичні системи можуть бути більш просунутими у здійсненні цифровізації, ніж демократичні держави. За цих умов важливо визначити характер пристосування державної політики до тенденції цифровізації, спроможність політичних акторів використовувати цифрові технології, створювати та поширювати контент для негайної вигоди численної онлайн-аудиторії, наявність політичні інституції в цифровій інфраструктурі для встановлення прямої комунікації із суспільством, а не через ЗМІ.

Цифрове поле, як частина цифрової політики, визначає процес формування цифрових політичних суб’єктів, створення цифрової інфраструктури та інтеграції фрагментованих спільнот. Процес цифровізації політики характеризується неспокійністю, нестабільністю та незавершеністю. Це пояснюється самою природою глобальної цифровізації, яка за своєю суттю є самовдосконаленням і самооновленням. У результаті формуються цифрові

політичні суб’єкти, які здатні до самоорганізації, постійного вдосконалення інструментів через створення більших спільнот та збільшення масштабів. Як наслідок, баланс сил у цифровому світі залежить від миттєвого додавання цих спільнот цифровими гравцями в політичні питання. Політична взаємодія зараз відбувається онлайн, що змушує всіх учасників сучасних політичних процесів створювати мережі та розробляти цифрові рішення політичних проблем. У зв’язку з цим актуальним для сучасної політичної науки є дослідження процедур формування нових цифрових політичних суб’єктів у контексті цифрової політики, особливостей розвитку мереж індивідами цифрової політики щодо влади, застосування влади до влади та складові цифровізації державної політики. [41].

Важливо розрізняти різні методи визначення цифрової політики. Цифрова політика розглядається як зростання значення цифрових технологій у політичних процесах. Таке розуміння не дозволяє описати механізми, викликані цифровізацією політики, оскільки базові цифрові здібності є звичним явищем у більшості країн планети. Діджиталізація політики в загальному розумінні – це створення цифрової політичної інфраструктури на основі впливу дискурсу глобальної цифровізації, який описує особливості взаємодії цифрових політичних суб’єктів із цією інфраструктурою та визначає особливості її формування. Цифровізація в цьому загальному сенсі створює нову форму політики: цифрову політику.

Цифровою політикою вважається практика організації політичних розмов за допомогою цифрових технологій, ця технологія відповідає за спосіб її використання. Цю політику проводять цифрові політичні актори, які використовують потенціал мереж, що розпадаються, об’єднуючи їх (утворюючи спільноти зі слабкими вертикальними зв’язками), щоб впливати на процеси розробки та впровадження політичних стратегій. Особливості трансформації політики, якій сприяє цифровізація, необхідно розуміти через цифровий політичний процес – процес перетворення / відображення значення в текст, який, у свою чергу, створює нові тексти та нові значення.

Серед основних факторів, залучених до процесу цифровізації державної політики в зарубіжних країнах, можна виділити такі категорії:

- активне впровадження нових знань і технологічних інновацій у всі сфери суспільного життя;

- створення громадянського суспільства та соціального партнерства в цифровій сфері;

- особливості ринкової економіки країни, що виявляються у стимулюванні в країні підприємництва, мобільності робочої сили, конкуренції на ринках;

- ступінь децентралізації влади та ефективність структурної та регіональної політики щодо покращення умов життя громадян з точки зору доходів і споживання;

- ступінь економічного розвитку країни, що впливає на здатність людей використовувати сучасні інформаційні та технологічні засоби;

Фонд сприятиме реалізації значущих соціальних проектів, які сприятимуть дотриманню соціальних принципів рівності та справедливості в цифровому світі. [36, с.4].

Особливості цифрових моделей публічного управління в значній мірі пов'язані з характером економічних відносин. Сьогодні існує кілька різних моделей цифрової політики. У моделі NeMT (Дж. Хофф, К. Шейлі) передбачається, що вплив один одного є постійним та інтенсивним, у результаті політичний дискурс, практика та технології змінюються з часом. В окремих теоретичних дослідженнях задокументовано вплив цифрових технологій на створення публічної сфери, передвиборну комунікацію та політичну участь, використання цифрових інструментів для взаємодії громадян і політичних сил (Р. Гібсон, Р. Косіара-Педерсен). , А. Фанг, А. Фланагін, М. Хансен,). Значні зміни, які відбудуться з політичними учасниками в результаті цифровізації, задокументовано в моделі кіберпартії (Х. Маджетс), описано формування сучасної мережевої структури партій. Також оновлена каскадна модель (Р. Ентман, Н. Ашер) описує процедуру поділу аудиторії та процедуру конструювання аудиторії навколо політичних діячів шляхом цифровізації.

Досвід Великобританії та Канади є в нагоді Україні, ці країни здійснили комплексну модернізацію системи державного управління з метою її відповідності вимогам цифрової економіки. У результаті у Великій Британії було започатковано стратегію модернізації державного управління, яка передбачала програму дій зі створення цифрової системи публічних послуг «електронні громадяни, електронний бізнес, електронний уряд». У контексті державного управління та структурування системи було сформульовано концепцію надання публічних послуг в інформаційному середовищі, що передбачає створення всіх електронних послуг з використанням Інтернету, мобільних технологій, цифрового телебачення чи сервісних центрів. Створення системи «Електронний уряд» (E-government) у Великобританії призвело до того, що вона стала однією з найвидатніших європейських країн у цьому відношенні. Метою масштабної програми модернізації та реконструкції державного управління з використанням інформаційних технологій є створення проектів «електронного уряду», які не лише надають інформацію громадянам, а й підвищують ефективність та результативність усього державного апарату. .

Результатом ефективного впровадження електронного уряду в Канаді стало надання послуг, вирішення транзакцій та взаємодія з громадянами та діловими партнерами в електронному форматі через «електронні кіоски» або Інтернет. Такий підхід до надання послуг популярний серед 95% канадців. Крім того, уряд Канади вважає, що передача послуг електронними засобами має доповнювати, а не замінювати традиційні методи зв’язку. Впровадження електронного уряду в Канаді підвищило ступінь співпраці між федеральним урядом і місцевими провінційними відомствами у сфері державного управління, а також підвищило прозорість і відкритість уряду для громадян, це стало можливим завдяки запровадженню звіти та пропозиції від будь-якої канадської урядової установи на її веб-сайті. Електронний уряд дозволив канадцям активніше брати участь у громадських справах і спостерігати за поведінкою державних установ, що позитивно вплинуло на розвиток громадянського суспільства [43, с. 14].

Аналіз сучасних теоретичних засад дозволяє сформулювати модель цифрової політики. Складовими моделі є цифрове поле, яке впливає на те, як відбуваються певні взаємодії між цифровими політичними суб'єктами та цифровою інфраструктурою; цифрова інфраструктура складається з низки технологій/інструментів для мережевої інтеграції; мережі користувачів складаються зі спільнот громадян, які вивчають і використовують цифрові технології/інструменти для досягнення спільних цілей, самоврядування; цифрові політичні актори використовують ці мережі для реалізації політики. [41, с.129]

В офлайн-контексті політичні діячі спілкуються із ЗМІ, тому що у них велика аудиторія – простий народ. Цифровізація призводить до того, що більшість аудиторії розбивається на менші групи, оскільки кожен може створити власну мережу та підключити до неї інших людей (за допомогою цифрових технологій). У результаті, щоб боротися за владу та вплив, цифрові політичні актори більше не повинні взаємодіяти з великою аудиторією через традиційні медіа, а натомість мають охоплювати все більше мереж.

Цифрова сфера держав впливає на методи побудови мереж. У зв'язку з цим дуже важливо відрізнити цифрову політику від значного цифрового недоліку (базові цифрові можливості доступні, але немає прикладів їх використання для створення децентралізованих мереж) і від невеликого цифрового недоліку (існує активна роль у створенні інноваційних способів використання). технології створення децентралізованих мереж). У зв'язку з цим важливо класифікувати цифрову політику та розрізняти два типи держав. Перший передбачає створення розгалуженої цифрової інфраструктури, яка охоплює численні мережі (політичні вороги, уряд і опозиція, політичні особи та активісти, усі ці мережі об'єднані цифровими технологіями, тобто всі політичні актори намагаються використовувати цифрові технології один одного.).

У державах першого типу відзначатиметься істотна зміна політичного ландшафту. Зрештою, впровадження цифрових технологій іноземними диджиталокіперами можливо.

Крім того, є держави, які побудували цифрову інфраструктуру іншого типу; склад мереж і їх структурний склад будуть різними. Зокрема, будуть сформовані передусім централізовані мережі, де невелика кількість цифрових політичних учасників може стати членами спільнот, а політичні взаємодії в першу чергу очолюються лідером держави. Або мережі, які пошкоджені та мають два-три компоненти, а решта цифрових політичних суб'єктів не пов'язані між собою. Крім того, через наявність цифрового розриву цифровим політичним суб'єктам доведеться використовувати мережі один одного для спілкування з громадськістю.

У державах другого типу не спостерігатиметься розмаїття цифрових політичних тем, а для представлення політичної взаємодії використовуватиметься спосіб представлення іноземних digitalatekeepers. [43, с.4].

Поряд із суспільством, яке розуміє використання цифрових технологій для участі в політиці, важливе значення мають конкретні особи, які роблять те саме, їхні причини, гонитва за «цифровим багатством» тощо. Зрештою, «цифрова політика розробляється акторами з різними цілями та намірами, які конкурують між собою» [44, с.4]

Як наслідок, використання цифрових технологій політичними учасниками для створення «смислів» за допомогою різних «практик» у цифровій сфері є значним. Тут необхідна ідея «структурування цифрових можливостей». Д. Крейс вважає, що ці структури впливають на рішення політика використовувати конкретні технології для досягнення стратегічних цілей. Різноманітність методів і форматів, які використовуються, є значною. Ці можливості доступні лише для кандидатів та їхніх помічників, якщо вони сприймають їх і мають можливість працювати в мережевому гібридному медіа-середовищі. [45, с. 49].

Ті самі численні методи, канали та формати також необхідні для того, щоб «збільшити вплив комунікації в складному, швидко мінливому середовищі» [46, с.3]

Однак консерватизм і традиційні підходи до комунікації про політику можуть стати проблемою для деяких політичних акторів. Структури цифрових можливостей є специфічними для кожного політичного актора, а також залежать від політичного клімату та символічних, матеріальних позицій, а також їх асоціації з цифровими медіа для стратегічних цілей.

Обговорюючи використання технологій політичними акторами, Дж. Хофф і К. Шилі зазначають, що динамічні відносини між мовними жанрами, які існують в результаті використання технологій у певних ситуаціях, а також різні голоси акторів, сприяють до зупинки потоку різниці та побудови центру. Це все приклади цифрових практик, які є похідними від використання цифрових технологій у певних ситуаціях. Політичні еліти, які, за словами П. Бурдьє, борються за символічне лідерство, створюють «дискурси, засновані на практиках», які вимагають нових поколінь програмного забезпечення (апаратного, програмного забезпечення) для виконання нових вимог.

Політичний конфлікт не обмежується використанням різноманітних інструментів, але також передбачає постійний розвиток технологій [47, с. 251].

Грунтуючись на суті президентських виборів у Франції 2012 року, дослідники детальніше пояснюють, як партії взаємодіють з виборцями в цифровому середовищі, визнаючи три різні ролі, які виборці можуть відігравати в цифровому просторі:

1) аудиторія (офлайн, традиційне значення);

2) прихильники чи друзі, які просто сприяють просуванню партії через лайки чи шеринги (очевидно, що жодна з цих організацій не має жодного впливу на політику партії);

3) Це цифрові активісти, які віддані справі та здатні взяти на себе роль службовців, вони беруть участь у політичних розмовах. Однак дослідники вважають, що цифровий активізм не є найпопулярнішою формою взаємодії між партією та громадськістю, хоча потенційно може мати вплив на політику [48, с. 94]. Наявність чи відсутність цифрової активності може вказувати на ступінь відкритості чи закритості політичних сил.

Вирішальними є не лише цифрові здібності, політичні знання, ресурси тощо, якими володіють громадяни, щоб брати участь у цифровій сфері, а й надихати політичні еліти залучати громадян до політики, таким чином роблячи їх співрозробниками політики. Крім того, наявність каналів для взаємодії громадян та еліт має вирішальне значення для цифрової політики та цифрової демократії [44, с. 14].

Повертаючись до важливості існування горизонтальних шляхів політичної взаємодії, варто зазначити, що їх мають розвивати як самі громадяни, які мають відповідні цифрові інструменти, так і політичні еліти, хоча остання, звісно, переоцінює важливість концепції, оскільки, за загальним правилом, реалізація політичними інститутами політичної взаємодії горизонтальних шляхів є «косметичною». Серед першочергових цілей Національної стратегії визначено створення середовища, яке сприятиме праву на об’єднання, посилення участі громадян у діяльності інститутів громадянського суспільства, зокрема такі:

- забезпечення працездатності системи громадянської освіти та моніторингу її ефективності;

- популяризація переваг створення інститутів громадянського суспільства для спільного вирішення громадянами питань, захисту прав та інтересів, здійснення практичної суспільно корисної діяльності, а також роз’яснення порядку реєстрації;

- скорочення складності та тривалості строків реєстрації, створення та припинення інститутів громадянського суспільства, підвищення оперативності документообігу в електронному вигляді, розширення обсягу суб'єкта реєстрації;

- створення єдиного підходу до визначення кінцевого благодійника для інститутів громадянського суспільства;

- реалізація ініціатив, спрямованих на покращення інфраструктури, у тому числі цифрової, яка сприяє ефективній діяльності інститутів громадянського суспільства, сприяє освітньому доступу цих закладів, комунікації з іншими інститутами та обміну ресурсами.

Також 21 липня 2021 року Кабінет Міністрів України схвалив Стратегію реформування державного управління в Україні на 2022-2025 роки, в якій зазначено, що «належне врядування є одним із найважливіших факторів розвитку економіки України та є необхідною умовою до європейської інтеграції Забезпечити ефективну діяльність Кабінету Міністрів України щодо формування державної політики в різних сферах, професійну, результативну та підзвітну. повинна бути створена система центральних органів виконавчої влади.

Відповідно до Угоди про асоціацію між Україною та Європейським Союзом, з одного боку, та Європейським співтовариством з атомної енергії, їх членами, з іншого боку, ця Стратегія виходить із спільної філософії: демократичних принципів, верховенства права та добра уряд. Стаття 3 Угоди про асоціацію описує належне врядування як один із основних принципів, що сприяють покращенню відносин між сторонами. Україна продовжуватиме політичні, економічні, законодавчі та інституційні зусилля, необхідні для успішної реалізації Угоди про асоціацію.

Крім того, в документі зазначено, що метою цієї Стратегії є створення в Україні компетентного сервісу та цифрової держави, що сприятиме захисту інтересів громадян на основі європейських принципів і методів.

Реформа системи державного управління розглядається в поєднанні з європейськими стандартами ефективного управління, які випливають з Програми підтримки вдосконалення врядування та управління та задокументовані в документі «Принципи державного управління».

Висновки до розділу 1

Розвиток цифрових технологій вважається найважливішим для впровадження цифрових технологій і цифрових інструментів у всі сфери життя. Це призводить до створення інноваційних продуктів, послуг і рішень, які мають підвищену здатність підвищувати ефективність, продуктивність і конкурентоспроможність у різних сферах. Він охоплює використання

обчислювальних і цифрових методів для створення нових технологій, платформ і систем, які задовольняють потреби користувачів і вирішують соціальні проблеми часу.

У результаті можна виділити такі характеристики міжнародних стратегій цифрової трансформації в контексті «Суспільства 5.0»:

1. Глобальний масштаб: у контексті «Суспільства 5.0» цифрова трансформація стає явищем, яке охоплює не лише окремі країни, а й увесь світовий ринок. Стратегії міжнародного бізнесу щодо цифрової трансформації спрямовані на вихід на різні ринки, формування партнерства через кордони та використання міжнародних ресурсів.

2. Різноманітність: стратегії міжнародного бізнесу повинні враховувати культурні відмінності та переваги кожної країни, з якою компанія взаємодіє. Розуміння культурних відмінностей і вміння адаптуватися до них сприяє конкурентній перевагі та збільшує ймовірність успіху з цифровими стратегіями.

3. Технологічні інновації: Суспільство 5.0 характеризується використанням передових технологій, таких як штучний інтелект, Інтернет речей, блокчейн тощо. Міжнародні стратегії цифрової трансформації повинні передбачати впровадження цих інновацій і створення нових цифрових рішень, адаптованих до потреб кожної країни.

4. Глобальна конкуренція: Умови «Суспільства 5.0» пропонують нові шляхи участі у світовій торгівлі. Стратегії міжнародного бізнесу повинні враховувати конкурентний ландшафт на ринку кожної країни та розробляти стратегію, яка має пріоритет.

5. Партнерство та співпраця: міжнародні бізнес-стратегії в контексті «Суспільства 5.0» спрямовані на формування партнерства та співпраці з іншими корпораціями, установами та країнами. Поєднання ресурсів, здібностей та інноваційних знань позитивно впливає на реалізацію цифрових проектів на міжнародному рівні.

Усі перелічені риси мають спільний знаменник, який полягає в необхідності комплексної та багатогранної міжнародної стратегії цифрової

трансформації, яка враховує унікальні характеристики кожного ринку, сприяє глобальній конкуренції та позитивно впливає на створення сталого та інноваційного бізнесу. в контексті «Суспільство 5.0».

Зараз Україна має скромний потенціал для просування цифрової трансформації. Проте ми визнаємо, що хоча процес відкриття нових можливостей заслуговує похвали, він також супроводжується значними викликами, які вимагають відповіді з боку держави через регуляторні інструменти.

Створення інформаційно-комунікаційних технологій, програмного забезпечення та супутньої інфраструктури є необхідним для розвитку цифрової державної політики з урахуванням найкращих світових практик. Проте його реалізація можлива за умов розвитку додаткових механізмів у кожному з векторів, які призначені для подальшого вивчення.

РОЗДІЛ 2
АНАЛІЗ ЦИФРОВОГО РОЗВИТКУ КРАЇН ТА СТРАТЕГІЙ ЇХ ЗАБЕЗПЕЧЕННЯ

2.1 Тенденції цифрової трансформації у світовій економіці

За останнє десятиліття цифровізація набула популярності в усіх частинах світу. Обробка та передача даних має глобальний масштаб через використання Інтернет-технологій, які не дотримуються національних кордонів. Тему цифровізації у світовій економіці досліджували численні економісти. Різні визначення класів цифровізації задокументовані в роботах Д. Тапскотта, Р. Маккуїна, Б. Карлссона, Б. Ван Арка та інших. Оцінкою тенденцій цифровізації займалися зарубіжні письменники Ф. Ніу, В. Пан, Т. Кім, Ю. Парк та ін. Окремі складові ініціативи українського уряду з цифровізації окремо розглянули Я. Байтельман, А. Бензар, В. Гамалій, Н. Краус, А. Мазаракі, А. Роскладка та інші, зокрема занепокоєння штучними нейронними мережами щодо управління цифровими активами та бізнесом [66], впровадження передових методів успішного цифрового економіки в цифровій політиці України [58].

Ефективне використання цифрових методів, методів і знань має стати невід’ємною частиною зростання економіки та продуктивності України.

Незважаючи на наявність значної кількості наукових досліджень щодо цифрової економіки, за останні роки не всі світові тенденції цифровізації були повністю розкриті. Важливим науковим завданням є визначення сучасних тенденцій, динаміки, особливостей і потенціалу цифрової трансформації в різних частинах світу. Розуміння еволюції цифровізації у світовій економіці допоможе Україні, яка відкрита для глобального економічного впливу, використовувати інструменти державної влади для максимізації вигод, уникаючи ризиків, пов’язаних із цифровою трансформацією країни.

Результати дослідження ЮНКТАД показують, що передача даних через кордони стала вирішальною для нової цифрової економіки. Нова глобальна

економіка зараз залежить від технологічних інновацій в Інтернеті. З 2005 по 2014 рр. середнє світове число користувачів Інтернету зросло в 4,24 рази, з 15,6% до 66,3% населення (рис. 2.1). У 2022 році очікується, що кількість людей, які користуються Інтернетом, становитиме майже 5,3 мільярда людей у всьому світі. Крім того, подібна картина зростання спостерігається в усіх класах людей і регіонах світу.

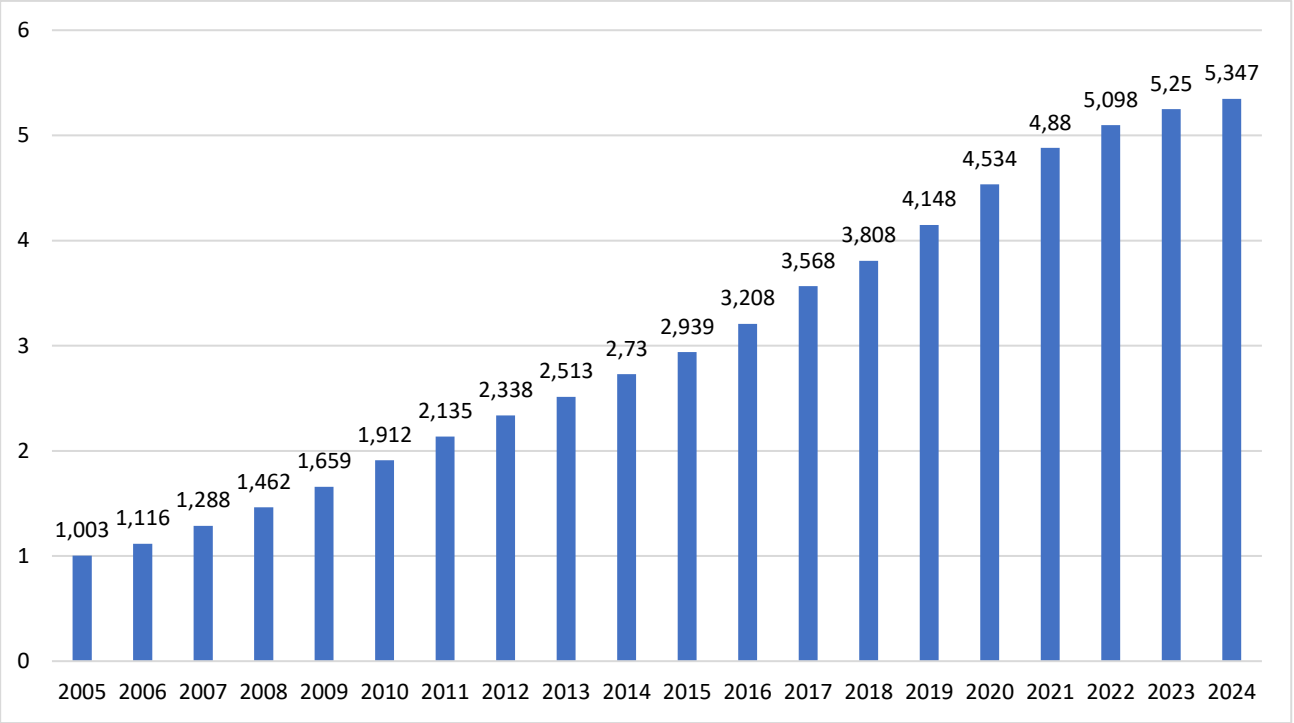


Рис. 2.1. Поширення Інтернету у світі, млн. користувачів

Примітка. Джерело: складено за [56]

У 2024 році приблизно 5,35 мільярда людей матимуть доступ до Інтернету, що становить 66,2 відсотка населення світу. За минулий рік кількість людей онлайн зросла на 1,8 відсотка, протягом 2023 року 97 мільйонів нових людей вперше вийдуть онлайн.

Крім того, на масштаби поширення Інтернету істотно впливає ступінь розвитку країн. Так, кількість користувачів Інтернету у 2022 р. становила 92,4% населення країн з високим рівнем доходу, тоді як лише 26,4% населення країн із низьким рівнем доходу мали доступ до Інтернету (табл. 2.1).

Таблиця 2.1

Користувачі Інтернету по країнах світу, %

Регіон	2019	2020	2021	2022	2023
Світ	53.7	59.6	62.6	66.3	70.0
Країни з високим доходом	88.3	89.5	91.0	92.4	90.0
Країни з доходом вище середнього	67.3	72.6	75.5	79.1	80.2
Країни з доходом нижче середнього	38.1	47.1	51.2	56.1	57.3
Країни з низьким доходом	17.0	19.9	22.5	26.4	27.2
Найменш розвинені країни	23.5	27.6	31.2	36.1	27.3
Європа	81.7	84.2	86.8	89.5	90.3
СНД	76.3	78.6	81.3	83.7	84.6
Америки	75.9	79.5	81.0	83.2	85.4
Арабські держави	55.2	61.6	65.8	70.3	75.3
Азійсько-Тихоокеанський регіон	48.9	56.6	60.1	64.3	66.4
Африка	27.7	31.8	35.3	39.7	40.1

Примітка. Джерело: складено авторами за [56]

Як видно з таблиці 2.1, бідні країни мають у 3,5 рази більше шансів стати успішними, ніж багаті країни. Серед континентів лідирують країни Європи, СНД і Америки, а аутсайдерами все ще вважаються країни Африки. Комісія зі сталого розвитку з широкосмугового доступу до Інтернету стверджує, що до 2025 року 75% населення світу матиме доступ до Інтернету, 60% з них будуть у країнах, що розвиваються, і 35% — у найменш розвинених країнах. Мобільний широкосмуговий Інтернет зараз популярний у всьому світі завдяки швидшій швидкості та більшому масштабу. З 2015 по 2022 рік кількість активних абонентів мобільного широкосмугового доступу зросла майже на 100% у всіх частинах світу. Особливо це стосувалося країн з низьким і низьким доходом. Сьогодні у світі налічується 5,16 мільярда користувачів Інтернету. Це означає,

що 70% населення світу має доступ до Інтернету. За рік кількість людей, які користуються Інтернетом, зросла на 1,9 % (рис. 2.2).

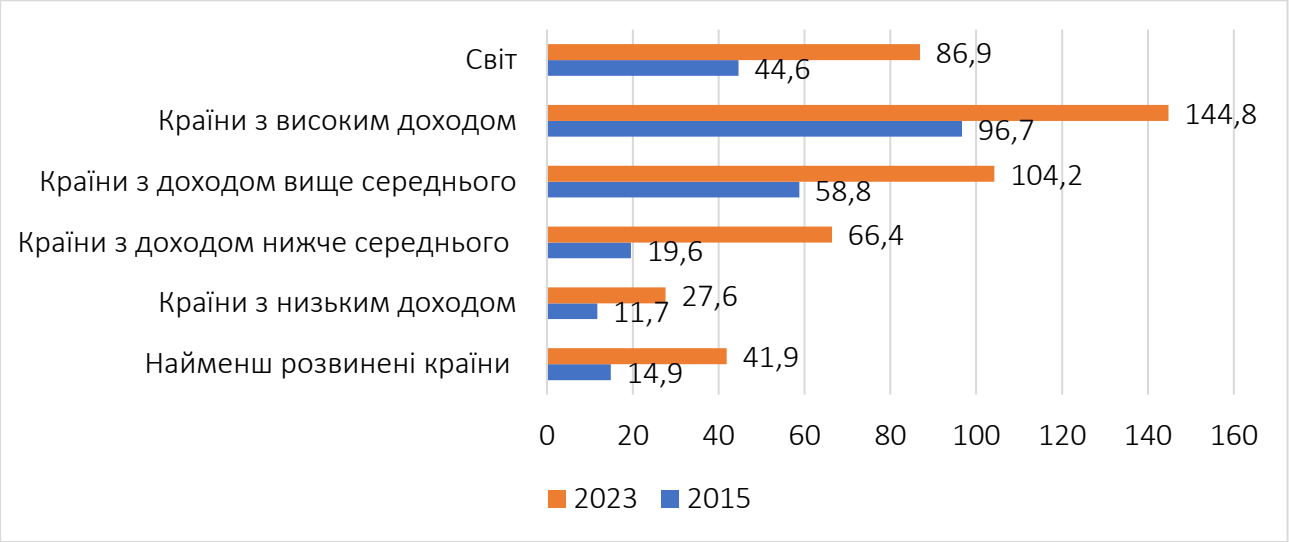


Рис. 2.2. Активні підписки на мобільний широкосмуговий доступ, за групами країн світу по рівню доходів (кількість на 100 осіб)

Примітка. Джерело: складено авторами за [56]

З малюнка видно, що нове місто менш популярне, ніж старе. 2.3, за кількістю активних підписок на мобільний широкосмуговий доступ на 100 осіб найбільше активних підписок мають країни Америки, Європи та СНД, найменше – країни Африки.

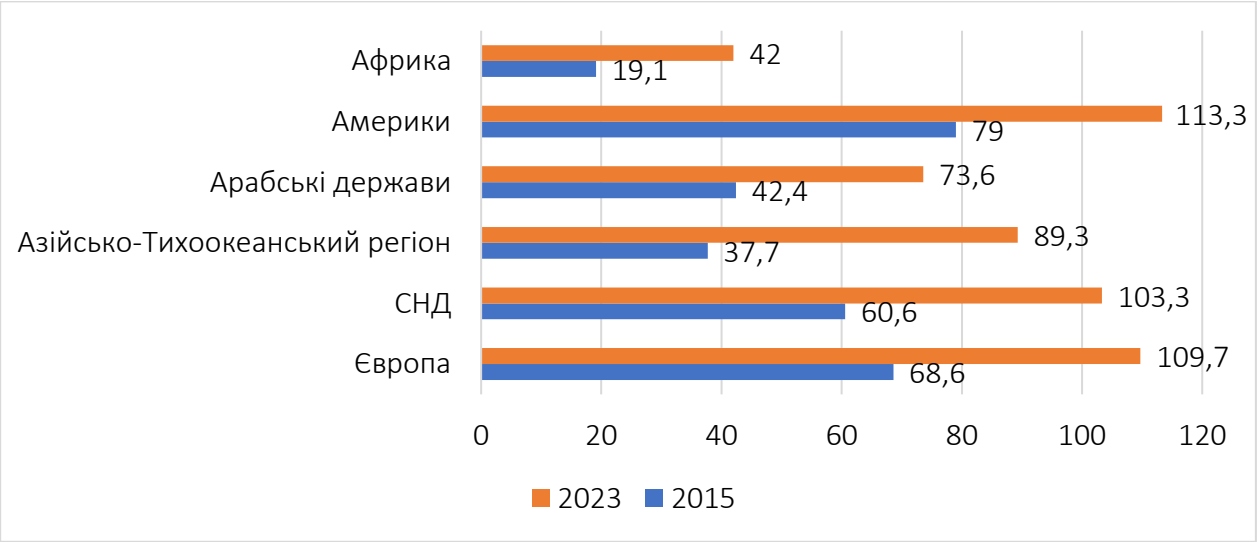


Рис. 2.3. Активні підписки на мобільний широкосмуговий доступ по регіонах світу

Примітка. Джерело: складено авторами за [56]

Смартфони мають вирішальне значення для доступу до бездротового Інтернету та передачі даних. Це особливо поширено в країнах, що розвиваються, де є фіксована кількість широкосмугового покриття та комп'ютери, але рідше ними користуються. Північна Америка та Європа були першими, хто мав смартфони, а потім Китай. Регіон Африки на південь від Сахари залишається винятком, станом на 2015 рік прогнозується збільшення кількості користувачів смартфонів.

Розглянемо ступінь покриття мобільних мереж у всьому світі в міських і сільських районах. Як наслідок, мережа 4G є найрозгалуженішою в усіх частинах світу, незважаючи на те, що найменш розвинені країни мають значний недолік покриття. У 2000 році загальне покриття мережі 4G у всьому світі становило 85%. У розвинених країнах він становив 97%, у країнах, що розвиваються, – 82%, у найменш розвинених – 41%. Крім того, покриття мережами 4G у містах значно більше, ніж у сільській місцевості. Зокрема, у 2000 році мережа 4G у сукупному охопленні всіх мереж у містах мала у всьому світі 95%, 100% – у розвинених країнах, 94% – у країнах, що розвиваються, 67% – у найменш розвинутих країнах, а також у сільській місцевості. територіях - 71% світу,86% - у розвинених країнах, 70% - у країнах, що розвиваються, і 27% - у найменш розвинених країнах. Мережі 2G і 3G все ще широко використовуються в країнах, що розвиваються і мають низький рівень розвитку.

Швидкість інтернет-з'єднання має вирішальне значення для здатності генерувати та використовувати дані. Якість зв'язку, судячи по швидкості з'єднання, має велике значення. Типова швидкість з'єднання є достатньою для основних дій, таких як перегляд веб-сторінок або електронна пошта, але не для відеовмісту чи відеодзвінків. Станом на липень 2023 року середня швидкість завантаження даних у світі зросла на 22,6% для фіксованого широкосмугового зв'язку та на 37,5% для мобільного зв'язку. Що стосується швидкості передачі даних, то за рік у світі вона зросла на 29,1 відсотка для фіксованого широкосмугового зв'язку та на 17,3 відсотка для мобільних телефонів.

Найвища пропускна здатність фіксованого інтернету в липні 2023 року була зафіксована в Сінгапурі, Гонконгу та Чилі, Україна посідає 66 місце у світовому рейтингу зі швидкістю лише 69,02 Мбіт/с. Найшвидший мобільний зв'язок у липні 2023 року був в ОАЕ, Катарі та Кувейті, Україна опинилася на 90 місці у світі зі швидкістю лише 25,87 Мбіт/с. З таблиці це видно. 2.2, розвинені країни передають лідерство у швидкості Інтернету країнам, що розвиваються, які побудували нові мережі передачі даних.

Таблиця 2.2

Лідери за швидкістю завантаження даних, липень 2023 р.

Зв'язок, мегабіт на секунду					
стаціонарний широкосмуговий			мобільний зв'язок, Мегабіт на секунду		
1	Сінгапур	247.44	1	ОАЕ	205.77
2	Гонконг (SAR)	242.99	2	Катар	186.35
3	Чилі	240.34	3	Кувейт	160.87
4	ОАЕ	238.28	4	Уругвай	149.08
5	Таїланд	211.28	5	Південна Корея	140.49
6	Сполучені Штати	207.32	6	Норвегія	122.72
7	Китай	193.66	7	Бруней	120.84
8	Данія	192.68	8	Ісландія	109.28
9	Іспанія	178.94	9	Нідерланди	106.27
10	Тайвань	177.43	10	Данія	101.19
66	Україна	69.02	90	Україна	25.87

Примітка. Джерело: складено авторами за даними [61]

Найпоширеніші способи використання Інтернету представлено в табл. 2.3. Як наслідок, розвинуті країни мають найвищий рівень ділової активності (Інтернет-банкінг, торгівля, професійні асоціації) та спілкування з державними установами; Африка має найбільшу участь у соціальних мережах, Африка має

найбільшу кількість завантажень програмного забезпечення, а Азія шукає роботу.

Таблиця 2.3

Види інтернет-діяльності осіб за групами країн, % населення

Інтернет-активність	Розвинені країни	Африка	Азія	Латинська Америка
Інтернет-банкінг	62.3	9.8	34.8	11.6
Надсилання або отримання електронної пошти	84.9	46.6	59.7	52.4
Отримання інформації про товари чи послуги	83.9	30.6	68	51.8
Отримання інформації від державних установ	55.1	17.6	20.9	23.2
Купівля або замовлення товарів чи послуг	53.9	14.6	29.1	13.1
Участь у соціальних мережах	70.4	86.3	87.2	79
Продаж товарів або послуг	16.8	3.5	6.4	9.3
Користування послугами для подорожей	55	7.5	25.2	28.4
Завантаження програмного забезпечення	19	62.8	41	20.7
Пошук роботи або надсилання/відправлення заявок на роботу	17.4	14.3	19.9	16.6
Участь у професійних мережах	21	5.9	6.4	0.7

Примітка. Джерело: складено авторами за даними [64]

Проаналізуємо еволюцію глобального інтернет-трафіку даних (рис. 2.4).

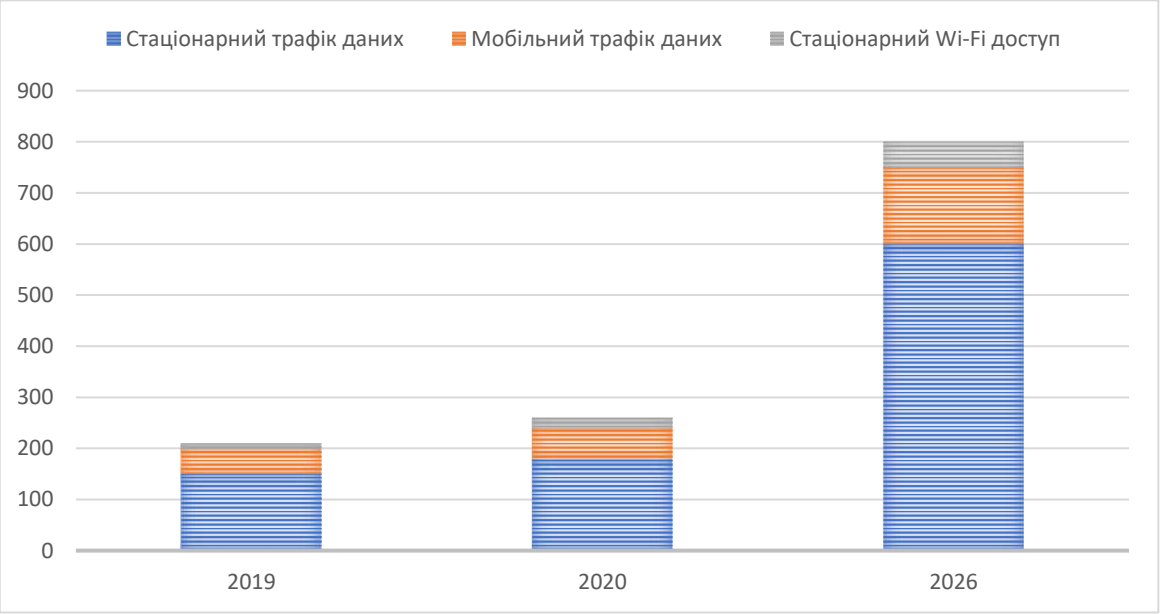


Рис. 2.4. Глобальний інтернет-трафік даних за видами, Екзабіт на місяць

Примітка. Джерело: [64].

На малюнку 2.4 видно, що світовий обсяг Інтернет-даних швидко зростає, і, як прогнозується, у 2025 році він сягне 780 ексабіт на місяць, що в 3 рази більше, ніж у 2020 році. Зазвичай Інтернет-трафік здійснюється через стаціонарні та мобільні телефони. , а також через стаціонарні маршрутизатори Wi-Fi. Лідерами за обсягом інтернет-трафіку є Азіатсько-Тихоокеанський регіон і Північна Америка, невелика його частка поділяється на Латинську Америку, Близький Схід і Північну Африку.

Дуже важко підрахувати кількість даних, які перетинають кордони – оцінки через проксі-сервери дуже невірні [60]. У літературі обговорюються проблеми вимірювання потоків даних через кордони та важливість розробки нових методів для покращення вимірювання цих потоків [53] замість міжнародного показника пропускної здатності, який часто використовується як альтернатива. З рисунка 2.5 видно, що Азійсько-Тихоокеанський регіон використовує глобальну пропускну здатність 542 Тбіт/с і є одноосібним лідером у світі. На другому місці – Європа та Америка. Аутсайдерами є African і Cisgenic.

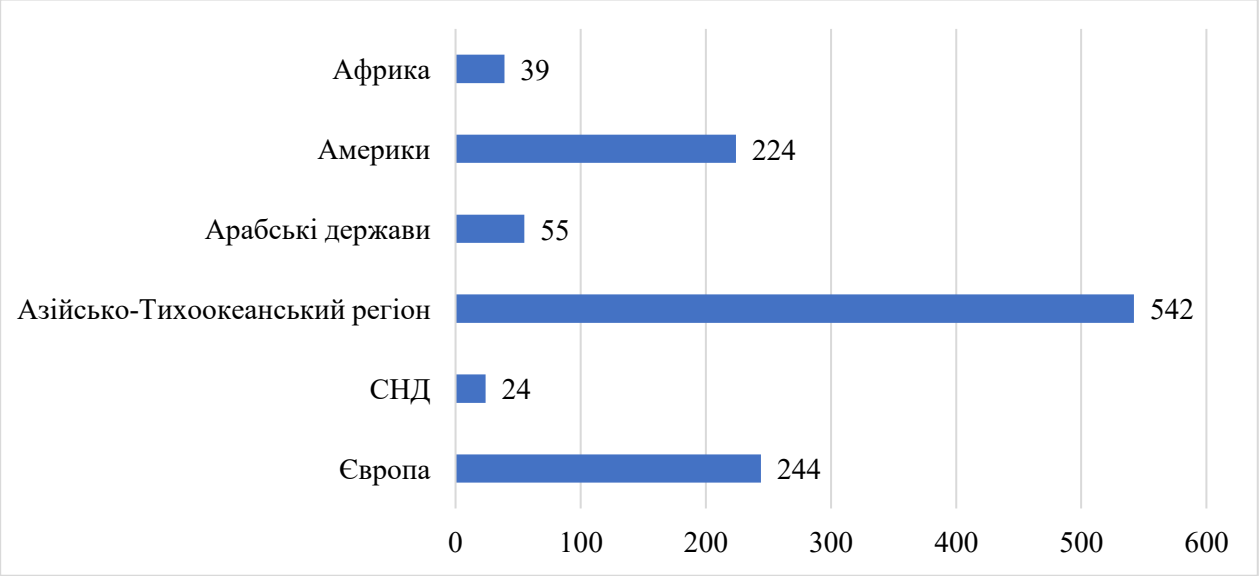


Рис. 2.5. Пропускна здатність у регіонах світу у 2023 р., Тбіт/сек

Примітка. Джерело: складено авторами за [56]

З огляду на отримані результати спотерігається тенденція збільшення пропускної здатності в усьому світі. Північна Америка, Європа та Азія є найпопулярнішими регіонами з точки зору пропускної здатності між регіонами.

Серед країн, що розвиваються, зв'язок між північчю і півднем очевидний між Америкою та Латинською Америкою, між цими регіонами спостерігається найвищий ступінь міжрегіональної взаємодії. На частку Китаю припадає 23 відсотки світової міграції даних через кордони, це пояснюється його асоціацією з іншими азіатськими країнами. На другому місці – США (12,8%). Зараз на країни Азії припадає приблизно половина загального глобального обсягу міграції даних, насамперед на Китай, В'єтнам і Сінгапур [63].

Глобальні цифрові платформи (GPP) мають зростаюче значення в усіх частинах ланцюжка даних. HCP відіграють особливу роль у процесі отримання великих обсягів даних, коли послугами користуються декілька користувачів. Це приносить їм користь, надаючи значну перевагу в конкуренції та дозволяючи їм отримувати більшу частину грошових вигод від цифрових технологій. Сукупний ефект мережі та доступу до даних, а також економія на масштабі може призвести до монополістичної тенденції та збільшення потужності найбільших у світі цифрових платформ (DP), головним чином розташованих у США та Китаї. Платформи досягли більшого успіху завдяки стратегічним придбанням інших компаній у різних галузях. Їхнє становище зросло під час кризи COVID-19. Розподіл 100 найкращих медичних працівників у світі станом на 2021 рік наведено в Додатку А.

Протягом 2017 року доходи провідних процесорів зросли, але це було посилено економічною кризою, спровокованою пандемією. Цю тенденцію не помітили інвестори, що відобразилося на фондових ринках: на Нью-йоркській фондовій біржі (NYSE) суттєво подорожчали акції американських компаній, на чолі з Apple, Microsoft і Alphabet (включаючи Google). Зростання цін на провідні процесори може свідчити про більшу різницю між цифровою та фізичною економіками. Також помітною є різниця в ринковій капіталізації цифрових гігантів Китаю та США.

Цифрові платформи збільшують свій вплив на ринку завдяки початковим придбанням і спеціальним інвестиціям у ШІ, що сприяє ефективній обробці даних і залучає нових учасників, тим самим генеруючи нові дані. Компанії та

країни, які мають ЦП, мають більше шансів очолити розробку штучного інтелекту та глобального управління даними, які мають вирішальне значення для цифрової економіки та майбутнього зростання всіх галузей.

Глобальний індекс штучного інтелекту, який базується на понад 100 показниках і був опублікований 28 червня 2023 року, містить список провідних лідерів у галузі штучного інтелекту зі США, Китаю, Сінгапуру, Великобританії, Канади, Південної Кореї, Ізраїлю, Швейцарія, Фінляндія. У рамках процесу злиття та поглинання, який відбувся в секторі штучного інтелекту протягом періоду часу 2016-2021, було укладено 308 угод на суму 28,4 мільярда доларів США.

Очікується, що до 2032 року світовий ринок штучного інтелекту матиме загальну вартість 2,745 мільярда, що порівняно з попередньою оцінкою в 177 мільярдів доларів у 2023 році. Зростання на 36,8 відсотка CAGR протягом прогнозованого періоду з 2024 по 2033 роки .

У 2024 році ринок штучного інтелекту перевищить 184 мільярди доларів США, що є значним збільшенням майже на 50 мільярдів доларів порівняно з 2023 роком. Очікується, що це тривожне зростання продовжуватиметься, а до 2030 року ринок становитиме 826 мільярдів доларів (рис. 2.6).

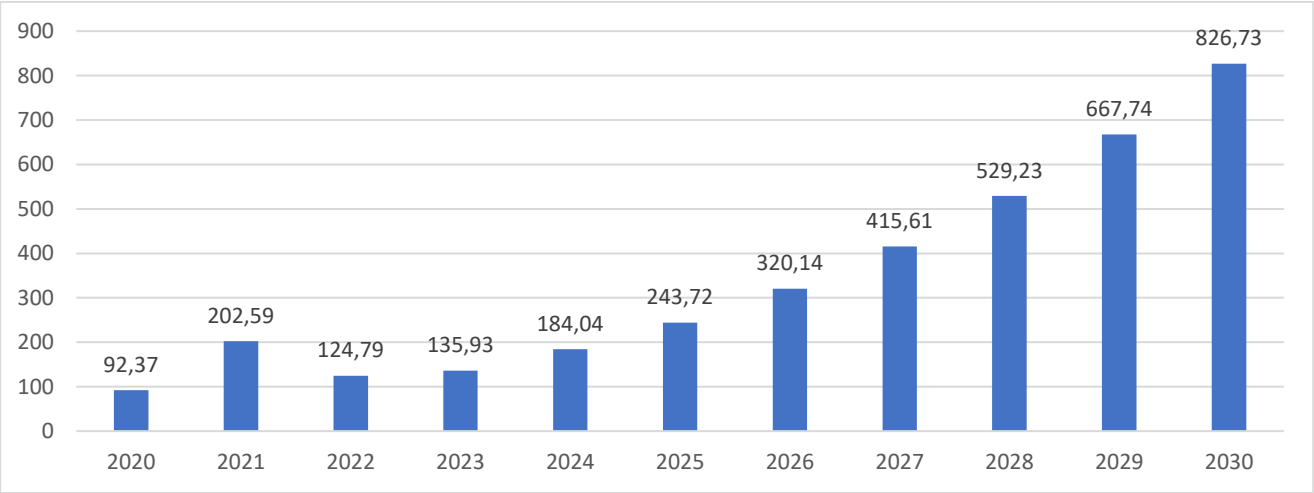


Рис. 2.6. Глобальний ринок штучного інтелекту, 2020–2030 рр., млрд дол. США

Примітка. Джерело: [64]

Управління даними продовжує залишатися найбільшою перешкодою для інфраструктури на основі ШІ. Цей конфлікт проявляється по-різному для компаній, які використовують ШІ. Деяким людям потрібна більш конкретна інформація, тоді як іншим важко підтримувати та систематизувати дані, пов’язані з їхнім бізнесом, які вже є. Великі міжнародні організації, такі як ЄС, США та Китай, мають правила щодо того, скільки даних можна архівувати за межами їхньої юрисдикції. Усі ці органи мають серйозний вплив на компанії, які використовують штучний інтелект.

Ймовірно, впровадження штучного інтелекту негативно вплине на США. Цей вплив може бути як позитивним, так і негативним, але він все одно повинен мати вплив на суб'єкта. Ротація робочої сили є корисною, якщо вона виконується правильно; це може швидко перевести працівників у більш продуктивні галузі з доданою вартістю, ніж у прості галузі праці. Завдяки цим змінам галузь матиме більш благотворний вплив на економіку. Фактично ШІ може підвищити продуктивність у США протягом 10 років. Очевидно, це залежить від багатьох факторів, включаючи ступінь потужності ШІ наступного покоління, складність завдань, які він може виконувати, і кількість працівників, яких переміщують.

Передбачається, що Інтернет речей стане основним методом збору даних у найближчому майбутньому з тисячами підключених електронних пристроїв. Дані можна збирати за допомогою таких підключених пристроїв: датчиків, лічильників, RFID та інших пристроїв, які можна вбудовувати в різні об’єкти, підключені до Інтернету. Ці пристрої використовуються в побуті. Зі зростанням поширеності оцифрування в глобальній економіці ланцюжок створення вартості даних просунувся в кількох країнах і тепер є більш розвиненим завдяки зниженню витрат і простішому використанню більш складних технологій, зокрема Інтернету речей [59]. Як наслідок, зростання популярності Інтернету речей призведе до збільшення майбутніх потоків даних через кордони [65].

До 2023 року кількість підключених пристроїв Інтернету речей у всьому світі зросте на 16,6% до 16,7 млрд [55]. Світовий ринок Інтернету речей оцінюється в 662,21 мільярда доларів. США в 2023 році і може зрости до 3,35

трильйона доларів. У США до 2030 року прогнозується щорічне зростання на 26,1 відсотка. Це вище середнього глобального зростання в 19,3%. Такі провідні компанії, як AT&T, Cisco, Siemens тощо, надають послуги, пов'язані з Інтернетом речей, такі як автомобільні рішення, керування з'єднаннями, контроль і передача даних, периферійні обчислення, цифрові близнюки та розумні міста. На Китай, США та Західну Європу припадає приблизно 75% загального обсягу Інтернету речей.

Рис. 2.7 показано розподіл доходів від Інтернету речей за регіонами світу з прогнозом на 2025 рік.

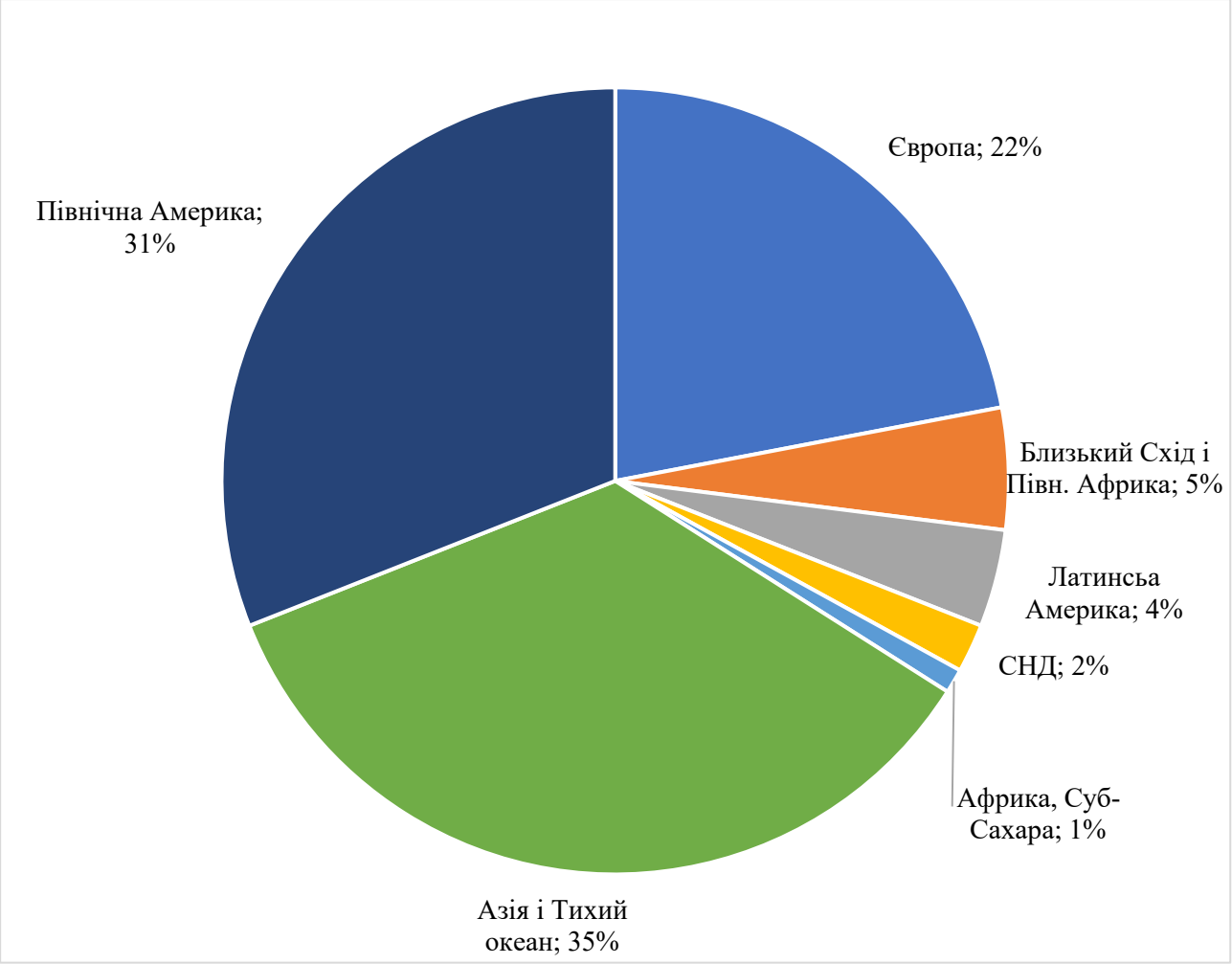


Рис. 2.7. Географічний розподіл доходів від інтернету речей, прогноз на 2025 р., %

Примітка. Джерело: [64]

До 2023 року різниця між компаніями та окремими особами, які використовують IoT, все ще буде досить очевидною. Прогнози ЮНКТАД показують, що промислово підключений Інтернет речей матиме більші темпи зростання. Це призведе до значних змін у структурі економіки та способах організації галузей.

2.2 Цифровий ландшафт України

Питання про те, наскільки український уряд розвинув цифрову платформу, є першочерговим для багатьох українських науковців. Т. Шталь [67] звертає увагу на зростання популярності цифрової економіки. У своїй статті Войтенко [68] досліджує позицію України щодо цих рейтингів, Індексу розвитку ІКТ, Індексу розвитку електронного урядування, Індексу глобальної кібербезпеки та Рейтингу цифрової конкурентоспроможності.AND. Дернова та Т. Боровик [68] зосереджуються на спільних рисах та трендах цифрової економіки України в умовах пандемії на основі рейтингу світової цифрової конкурентоспроможності IMD та індексу готовності до мереж, обидва з яких враховують субіндекси.

М. Рощук [69] досліджує позиції України в Індексі розвитку електронного урядування, Індексі готовності мереж WEF/WITSA та глобальному рейтингу цифрової конкурентоспроможності IMD. Галущак О., Галущак М., Машлій Г. [71] звертають увагу на еволюцію процесу цифрової трансформації в Україні на основі світового рейтингу цифрової конкурентоспроможності IMD. Безрук Д. [67] виділяє наступні індекси цифровізації в економіці: The Global Innovation Index, Digital Economy and Society Index, ICT Development Index, Network Readiness Index, Digital Evolution Index, Boston Consulting Group's Electronic Intensity. Індекс та індекс впровадження цифрових технологій.

Подольчак Н., Білик О., Левицька Я. та ін. [78] зосереджуються на готовності мережі до розвитку ІКТ та цифрової еволюції. [78] зосереджені на Індексі готовності мережі, Індексі глобальних інновацій, Індексі розвитку ІКТ та Індексі глобальної конкурентоспроможності. Polous O. [79] для оцінки

використовує глобальний рейтинг цифрової конкурентоспроможності IMD, WEF/WITSA Network Readiness Index, UNCTAD B2C E-Commerce Index та Digital Economy and Society Index. Семеног А. [80] вивчає глобальний індекс цифрової конкурентоспроможності IMD, індекс впровадження цифрових технологій, індекс глобального підключення та індекс зручності цифрового бізнесу.

Руденко М. [81] виділяє такі метрики потенціалу цифрової економіки: Digital Economy and Society Index, Digital Evolution Index, ICT Development Index, Global Innovation Index, Network Readiness Index, e-Intensity Boston Consulting Group. , а також глобальний індекс цифрової конкурентоспроможності IMD.

Незважаючи на те, що дослідженню позиції України в міжнародних рейтингах цифрової економіки присвячено значну кількість наукових досліджень, у більшості з них не розглядаються субіндекси чи тенденції їх розвитку. Однак розпізнавання тенденцій субіндексів може допомогти оцінити та визнати переваги та недоліки процесів цифровізації в Україні, а також може надати інформацію про потенціал трансформації бізнес-процесів у країні.

Наразі не існує жодного індексу, який би комплексно вимірював цифровий розвиток країни. Як наслідок, для оцінки різних компонентів цифрової економіки зазвичай використовується кілька показників (наприклад, нещодавнє дослідження, яке аналізує дані досліджень, показало, що рейтинг глобальної цифрової конкурентоспроможності IMD є найпопулярнішим інструментом, який використовується для оцінки ступеня цифровізації країни.

Індекс цифрової конкурентоспроможності визначається Швейцарським інститутом розвитку менеджменту. Оцінка базується на трьох основних категоріях, кожна з яких має три підкатегорії: знання (талант, освіта та підготовка, наукова спрямованість), технології (нормативна база, капітал, технологічна інфраструктура) та готовність до майбутнього (адаптивне ставлення, бізнес-гнучкість, IT-інтеграція).

На рисунку 2.8 показано еволюцію рейтингів для окремих країн з 2017 по 2021 рік (оскільки індекс для України не оцінювався у 2022 році, використовувався рейтинг глобальної цифрової конкурентоспроможності IMD).

З рисунка 2.8 можна зробити висновок, що протягом досліджуваного періоду більшість країн не зазнали істотних змін у своєму рейтингу. Проте п'ятирічний спад спостерігається у Фінляндії, Польщі (у 2021 році), Болгарії (у 2021 році) та Хорватії (у 2022 році). Натомість у 2021 році Україна здобула вищий рейтинг.

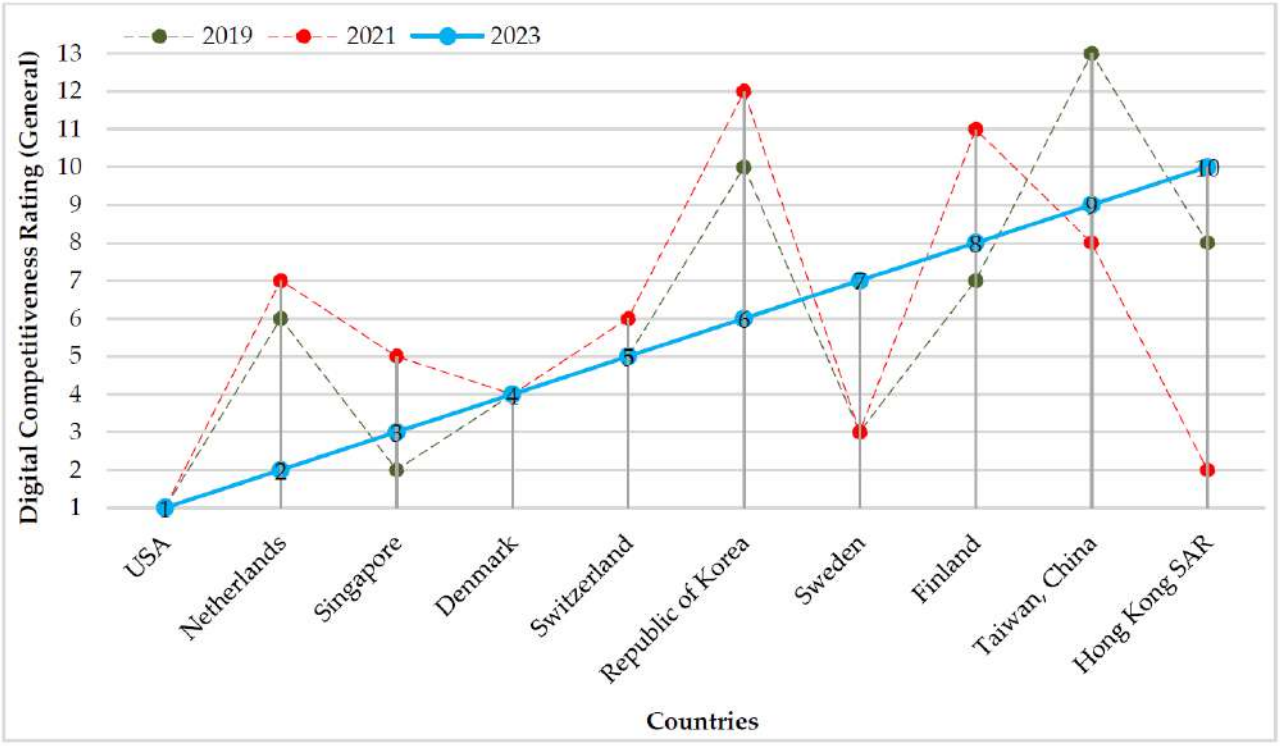


Рис. 2.8. Динаміка зміни рейтингу цифрової конкурентоспроможності (загальної) країн світу (ТОП-10), IMD World Digital Competitiveness Ranking 2023 у 2019, 2021, 2023 роках

Примітка. Джерело: [71 - 75]

Крім того, за останній рік ландшафт кіберзагроз продовжував розвиватися в небезпечний і складний простір. Зловмисники в усьому світі стають винахідливішими та більш підготовленими, вони застосовують дедалі складніші

тактики, методи та інструменти, які кидають виклик найдосвідченішим експертам у світі з кібербезпеки.

Примітною є продемонстрована Україною стабільність у міжнародних рейтингах кібербезпеки, зокрема в Global Cyber Security Index (GCI) та National Cyber Security Index (NCSI).

Україна посідає 76 місце серед 182 країн у GCI, що свідчить про значне зростання розвитку кібербезпеки України. [71 - 75].

У NCSI Україна посідає 13 місце із загальним показником 80,83 бала, що свідчить про високий рівень розвитку країни щодо кібербезпеки [85].

Динаміка позиції: з 2019-2023 років Україна посилить свої позиції в цих рейтингах, що свідчить про цінність заходів у сфері кібербезпеки. Проте аналіз профілю кібербезпеки України в Global Cyber Security Index (GCI) демонструє низький кіберзахист країни (рис. 2.9).

Рис. 2.9 Аналіз профілю України Глобальному Індексі кібербезпеки (GCI) у 2024 р.

Примітка. Джерело: побудовано на основі [71-75]

Як видно з рисунка 2.9, сфера кібербезпеки в Україні демонструє позитивні тенденції, але для досягнення максимально можливої безпеки необхідно впроваджувати додаткові заходи та стратегії. Окреслені стратегії наразі активно впроваджуються в Україні щодо кібербезпеки. І навпаки, у сферах співпраці, розвитку потенціалу, організації та технічної допомоги між європейськими та іншими країнами існує значна різниця.

У підсумку, враховуючи проведені теоретичні та аналітичні дослідження, рекомендується зосередитися на пріоритетних напрямках розвитку інформаційної структури протидії кіберзагрозам:

- підвищуючи освітній рівень і професійний розвиток, програми кібербезпеки повинні розширюватися на кожному рівні освіти та підтримуватися професійними організаціями.

- міжнародне співробітництво здійснюється через участь у міжнародних ініціативах та обмін досвідом з іншими країнами.

- стимулювання інвестицій у технологічні інновації та інфраструктуру для забезпечення ефективного захисту інформаційних систем.

2.3 Аналіз впровадження та реалізації міжнародних стратегій кіберзахисту

Зараз кібербезпека має важливе значення для цифрового життя в підключеному світі. З розвитком технологій організації все частіше звертаються до цифрових систем. Як наслідок, захист конфіденційної інформації, збереження довіри клієнтів і забезпечення безперервності бізнесу тепер вважаються головними цілями. Зараз кібератаки є звичайним явищем у бізнесі, ця проблема завдала збитків у трильйони доларів. Що погіршує ситуацію, конфлікт між Україною та Росією призвів до цих проблем через серію масштабних кібератак, мотивованих політичними мотивами [89].

У 2022 році галузь матиме найбільший відсоток кібератак у порівнянні з іншими галузями в усьому світі. Протягом досліджуваного року кібератаки на

виробничі компанії становили майже 25% від загальної кількості кібератак, фінансові та страхові компанії – майже 19% від загальної кількості кібератак, професійні, ділові та побутові послуги – приблизно 14,6% від загальної кількості кібератак. кібератаки (рис. 2.11) [90].

Багато країн постійно оновлюють свої національні стратегії кібербезпеки (NCS) [9], щоб вони відповідали мінливому ландшафту. Наявність національної стратегії кібербезпеки (NCS) є корисною для стану кібербезпеки в країнах, але регулярні оновлення необхідні в міру розвитку ландшафту загроз і пріоритетів. Країни зазвичай мають 4-5 років для оновлення NCS. Деякі країни мають більш довгострокові зобов'язання, які можуть тривати десятиліття чи більше [91].

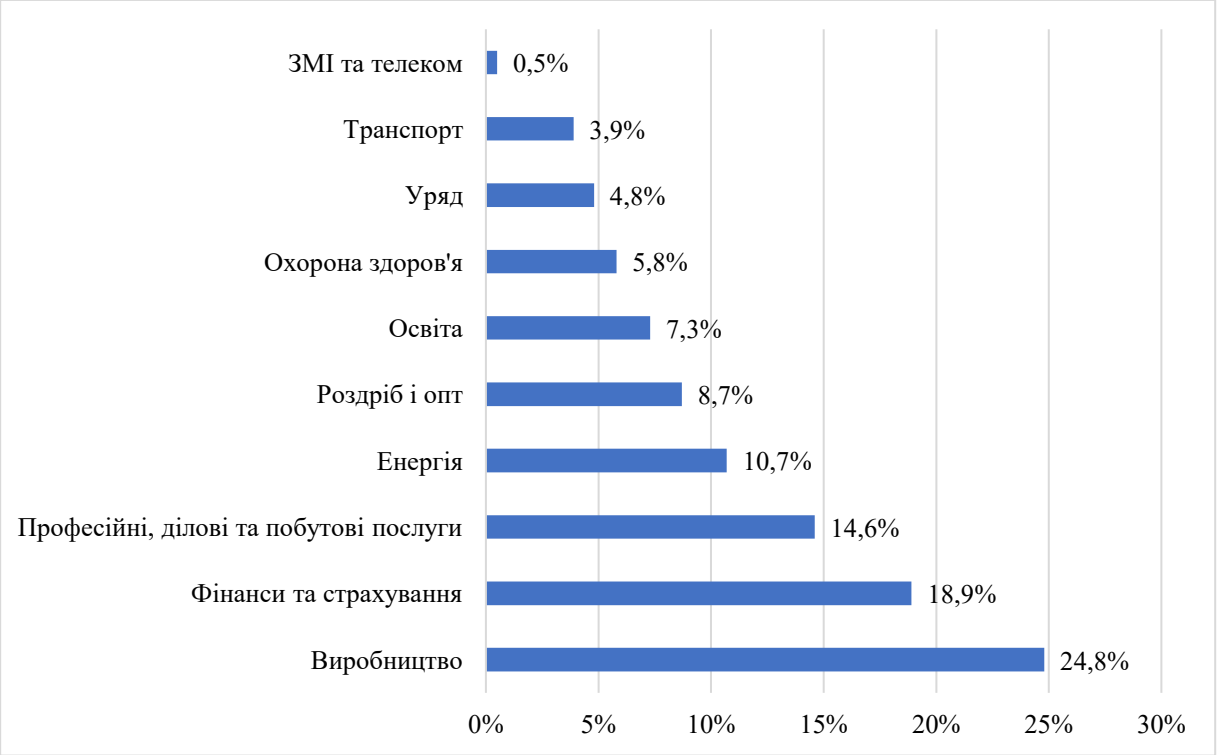


Рис. 2.11. Розподіл кібератак по галузях в світі у 2022 році, %

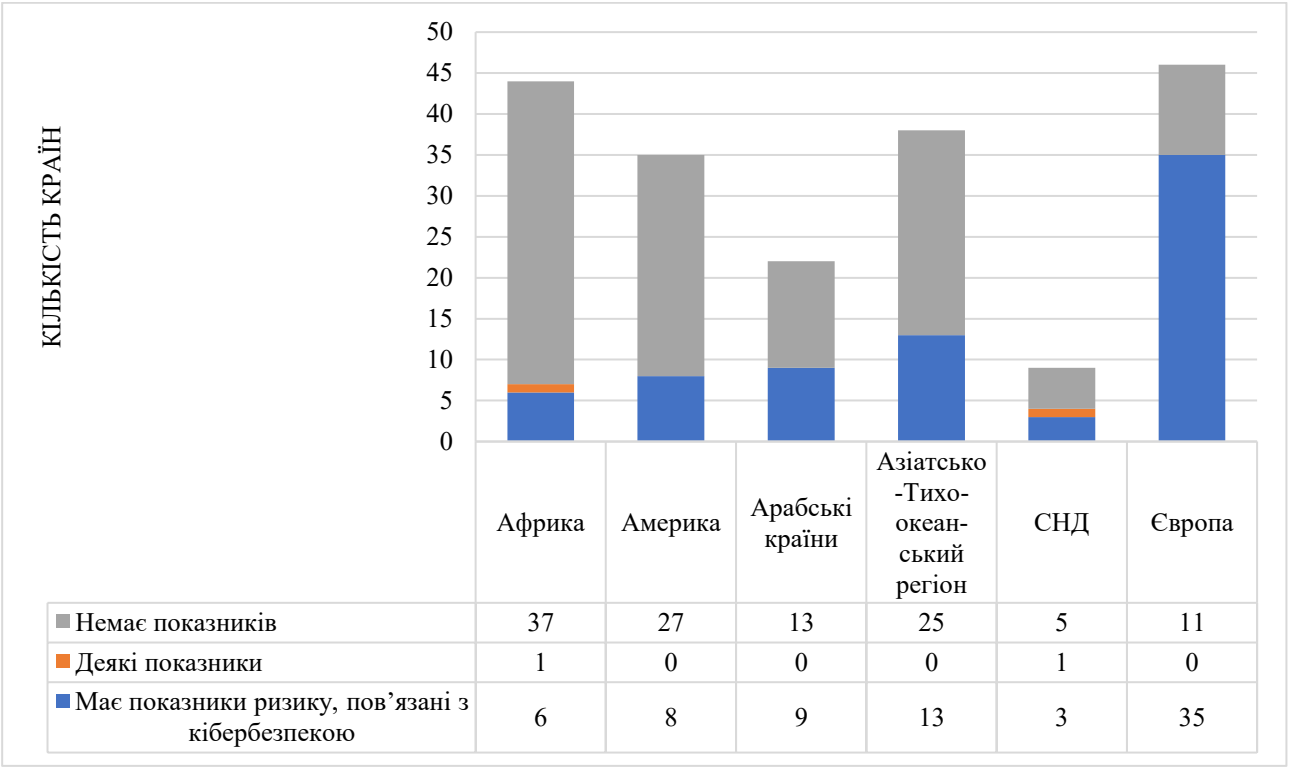
Примітка. Джерело: [91]

Зі 127 країн, які мають національну стратегію кібербезпеки, яка є поточною, існує більше п'яти років або знаходиться на стадії розробки, 60 країн продемонстрували прогрес у встановленні більш конкретних цілей шляхом

модифікації та розробки нових стратегій щодо кібербезпеки або шляхом оновлення своїх плани.

Важливість кібербезпеки в критичній інфраструктурі та стабільності відображається як у бюджеті, так і в стратегії національної безпеки. Національні стратегії кібербезпеки, швидше за все, стосуватимуться необхідної інфраструктури та/або стійкості кіберпростору. Однак деякі країни не використовують жодного з них.

Наявність національної стратегії кібербезпеки є вигідною в короткостроковій перспективі, але необхідні регулярні оновлення та перегляди. Багато країн, які мають NCS, не оцінюють і не коригують свої стратегії безпеки на регулярній основі у відповідь на зміну ландшафту загроз і пріоритетів у кіберпросторі. NCS 98 країн із оновленими NCS включає лише 60, які включають життєвий цикл оцінювання як частину їх стратегії (рис. 2.12) [93].



	Африка	Америка	Арабські країни	Азіатсько-Тихо-океан-ський регіон	СНД	Європа
Немає показників	37	27	13	25	5	11
Деякі показники	1	0	0	0	1	0
Має показники ризику, пов'язані з кібербезпекою	6	8	9	13	3	35

Рис. 2.12. Показники для оцінки ризику, пов'язаного з кіберпростором, на національному рівні

Примітка. Джерело: [93]

Як видно з рисунка 2.12, найбільший ступінь ризику, пов'язаного з кіберпростором, спостерігається в Європейському Союзі, який сформулював стратегічний документ – Цифровий компас 2030 [83], який описує орієнтований на людину, стійкий і процвітаючий цифровий майбутнє. Він класифікує чотири регіони з конкретними цілями: кваліфіковане населення та висококваліфіковані цифрові професіонали, безпечна та ефективна цифрова інфраструктура, трансформація бізнесу та цифровізація державних послуг.

Проте в контексті масштабної цифровізації всіх сфер життя варто розглянути й іншу сторону цих процесів, а саме стрімке зростання кібернебезпек.

З 2016 року Міністерство закордонних справ Естонії очолює програму, яку підтримує Estonian Development Cooperation and Humanitarian Aid. Ця програма спрямована на оцінку кібербезпеки країни та надання потенційних джерел і критеріїв для оцінки. Національний індекс кібербезпеки (NCSI) — це інструмент, який забезпечує оцінку кібербезпеки країни та дозволяє потенційно впроваджувати джерела та критерії для оцінки. Як наслідок, NCSI є ресурсом, який містить загальнодоступні матеріали та інструменти для розвитку кіберпотенціалу країни з точки зору потенційних застосувань та переваг [86].

У таблиці 2.4 наведемо результати Національного індексу кібербезпеки та Індексу цифрового розвитку країн ЄС та України за 2023 рік.

Таблиця 2.4

Результати Національних індексів кібербезпеки та індексів Цифрових рівнів розвитку країн ЄС та України за 2023 р.

Позиція	Країна	Національний індекс кібербезпеки (NCSI)	Цифровий рівень розвитку (DDL)	Розрив (NCSI від DDL)
1	2	3	4	5
1.	Бельгія	94,81	74,07	20,74
2.	Литва	93,51	67,34	26,17
3.	Естонія	93,51	75,59	17,92
4.	Чеська Республіка	90,91	69,21	21,70
5.	Німеччина	90,91	80,01	10,90

Продовж. табл. 2.4

1	2	3	4	5
6.	Румунія	89,61	59,84	29,77
7.	Греція	89,61	64,02	25,59
8.	Португалія	89,61	68,46	21,15
10.	Іспанія	88,31	72,21	16,10
11.	Польща	87,01	65,03	21,98
12.	Австрія	85,71	75,76	9,95
13.	Фінляндія	85,71	78,35	7,36
15.	Франція	84,42	77,29	7,13
16.	Швеція	84,42	81,51	2,91
17.	Данія	84,42	82,68	1,74
18.	Хорватія	83,12	64,63	18,49
19.	Словаччина	83,12	65,44	17,68
20.	Нідерланди	83,12	81,86	1,26
23.	Італія	79,22	67,26	11,96
25.	Латвія	75,32	66,23	9,09
26.	Ірландія	75,32	75,18	0,14
28.	Болгарія	74,03	62,06	11,97
37.	Угорщина	67,53	64,25	3,28
38.	Словенія	67,53	69,74	-2,21
41.	Кіпр	66,23	68,83	-2,60
43.	Люксембург	66,23	78,40	-12,17
76.	Мальта	50,65	71,74	-21,09
24.	Україна*	75,32	55,96	19,36

* не входить до країн ЄС

Примітка. Джерело: [86]

З таблиці 2.4 видно, що перші вісім позицій у світі за ступенем кібербезпеки займають країни ЄС, зокрема Бельгія, Лівія, Естонія, Чехія, Німеччина, Румунія, Греція та Португалія.

NCSI кількісно оцінює ступінь кібербезпеки країни, її готовність до уникнення кібернебезпек і її здатність протистояти кіберзлочинам, катастрофам і великим кризам. Місія NCSI полягає у створенні комплексного інструменту вимірювання кібербезпеки, який поширює точну та доречну інформацію про національну кібербезпеку.

NCSI зосереджується на вимірних аспектах кібербезпеки, запропонованих федеральним урядом, і намагається визначити, які політики та стратегії слід запровадити, щоб покращити кібербезпеку країни.

Висновки до розділу 2

Результати дослідження свідчать про те, що еволюція цифровізації у світовій економіці є значною та демонструє різні моделі в різних регіонах світу. Кількість людей, які користуються Інтернетом, стрімко зросла в усіх частинах світу, збільшившись у 4,2 рази від загальної кількості населення в 2005-2018 роках, з прогнозованим зростанням до 2025 року. Бідні країни мають у 3,5 рази більшу схильність до успіху за цим показником, ніж багаті країни.

Використання мобільного широкосмугового зв'язку в усьому світі зросло на дві третини за останнє десятиліття, у той час як країни з низьким рівнем доходу значно поступаються країнам з високим рівнем доходу з точки зору широкосмугового доступу. Одним із найважливіших факторів наявності бездротового доступу до Інтернету є наявність смартфонів у населення, це вартість доступу, яка є непомірно високою в найменш розвинених країнах.

У всіх регіонах світу є мережі 4G, однак найменш розвинені країни значно відстають, все ще використовують 3G і навіть 2G. Крім того, покриття мережами 4G у містах значно більше, ніж у сільській місцевості в усіх регіонах.

Швидкість глобального завантаження даних зростає як для фіксованої смуги пропускання, так і для мобільного зв'язку. Лідерство за цим показником пояснюється наявністю нової високошвидкісної інфраструктури передачі даних, тому розвинені країни часто менш розвинені, ніж країни, що розвиваються.

Розвинені країни мають найвищий рівень послуг онлайн-бізнесу та електронного уряду. Азія є першою за використанням соціальних мереж і онлайн-пошуку роботи, тоді як Африка має найвищий відсоток завантажень програмного забезпечення. Азіатсько-Тихоокеанський регіон є найпопулярнішим споживачем міжнародної смуги пропускання.

Цифровізація каталізує швидке розширення цифрових платформ, і ці платформи матимуть різноманітні компанії в різних галузях. Зростаюча популярність провідних ЦП може свідчити про зростаючу різницю між

віртуальною та реальною економіками. Орієнтовна ринкова вартість китайських компаній цифрових технологій нижча, ніж американських.

Розвиток штучного інтелекту та Інтернету речей прискорився, а лідируючі позиції в цих сферах зберігають США та Китай. Ланцюжок створення вартості для даних розвивається в усьому світі, з різними етапами в різних країнах. Визначення поняття національного суверенітету в контексті глобальної цифрової економіки потребує перегляду. Проблемою, пов'язаною з додатковими дослідженнями, є питання вимірювання обсягу даних, що надходить, цінності даних і того, як розрізнити необроблені дані та цифрові продукти (цифровий інтелект, який є результатом обробки даних).

Тому у другому розділі розглядаються підходи науковців до визначення міжнародних показників для вимірювання ступеню технологічного розвитку країн. Було досліджено, які з цих показників оцінюють якість цих показників для України. Глобальний рейтинг цифрової конкурентоспроможності IMD був ретельно вивчений, що дозволило як позицію України в міжнародному рейтингу, так і провести аналіз окремих субіндексів і субфакторів. Це призвело до визначення можливостей і викликів у цифровізації України. Отримані результати можуть бути використані при розробці стратегії щодо конверсії бізнес-процесів, визначенні пріоритетності напрямків, потенційних перешкод і переваг цифрових технологій у діяльності компаній.

РОЗДІЛ 3
ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ СТРАТЕГІЇ ЦИФРОВОГО РОЗВИТКУ УКРАЇНИ

3.1 Перспективні напрями реалізації стратегії цифрового розвитку України

Останнім часом актуальним сьогодні стало питання цифровізації економіки. У відповідь на цифрові технології та їх розвиток відбуваються масштабні трансформації не лише в технологічній сфері, а й у соціальних сферах.

Зараз у світі є цифрова інфраструктура в усіх сферах соціальної та економічної діяльності. Спочатку це пов'язано з глобалізаційними аспектами структурної перебудови країни. Прогрес цифровізації незмінно залежатиме від цілей розвитку держави. Лише за підтримки держави цифрову економіку можна розвинути в будь-якій країні. Це ставить перед державою значні виклики, які можна адекватно вирішити шляхом цифрової трансформації державного управління. Однак концепція переходу держави на цифрову платформу сьогодні має низку обмежень і небезпек, які необхідно усунути. Також важливо адаптуватися до нових принципів цифрової економіки та гармонізувати та адаптуватися до урядових та бізнес-структур країни. Останнім часом цифрова торгівля як частина цифрової економіки позитивно вплинула на сталий розвиток і глобалізм. Успішна стратегія розвитку цифрової економіки призведе до швидкої, сталої та оцифрованої економіки, це документ, який сприяє узгодженню влади та бізнес-структур.

За даними Українського інституту майбутнього [3], для досягнення цієї мети необхідно інвестувати 70 млрд $ в цифрові технології протягом наступних десяти років (табл. 3.1).

За даними Українського інституту майбутнього, "Економічна стратегія України - 2030" окреслює два потенційні шляхи розвитку цифрової економіки України. Ці сценарії залежать від оцінки важливості та нагальності

впровадження суттєвих змін у традиційній економіці: інерційний (еволюційний) сценарій та цільовий (вимушений) сценарій.

Таблиця 3.1

Перспективи цифровізації економіки України у 2021-2030 роках

Індикатори	2021 р.	2025 р.	2030р.	Всього за 2021-2030рр.
Інвестиції в цифрову інфраструктуру, млрд дол.	0,7	3	6	16
Інвестиції в діджиталізацію бізнесу, виробництва, та промисловості, млрд доларів США.	1,5	5	14	70
Підвищення продуктивності завдяки діджиталізації, %.	1,1	1	13	
Додатковий ВВП, створений завдяки діджиталізації, млрд. доларів США.	17	93	280	1 260
Додатковий ВВП, %.	11	44	95	240
Кількість нових вакансій (без урахування експортної ІТ- індустрії), тисяча людей	150	300	700	
Частка цифрової економіки в Україні (у загальному ВВП), %.	3	15	65	

Примітка. Джерело: створено автором на основі [3]

Інерційний сценарій передбачає збереження історичних закономірностей, зокрема поступове впровадження технологій, діджиталізацію економіки та розвиток людського капіталу. За цим сценарієм очікується, що економіка України залишатиметься неефективною, трудова міграція триватиме, а вітчизняне виробництво намагатиметься зберегти конкурентоспроможність на міжнародних ринках.

І навпаки, цільовий сценарій передбачає швидку трансформацію української економіки протягом 5-10 років зі значною часткою цифрової економіки, яка становитиме до 65% ВВП. Досягнення ВВП у 1 трильйон доларів США є досяжним для України, але потребує інтеграції інформаційних технологій в усі сектори економіки [3].

На рисунку 3.1 показано, що до 2030 року цифрові продукти становитимуть 65% всієї економіки. Однак, щоб досягти цього, українському

ринку необхідно до 2030 року виробити та спожити інформаційних продуктів на суму приблизно 16 мільярдів доларів.

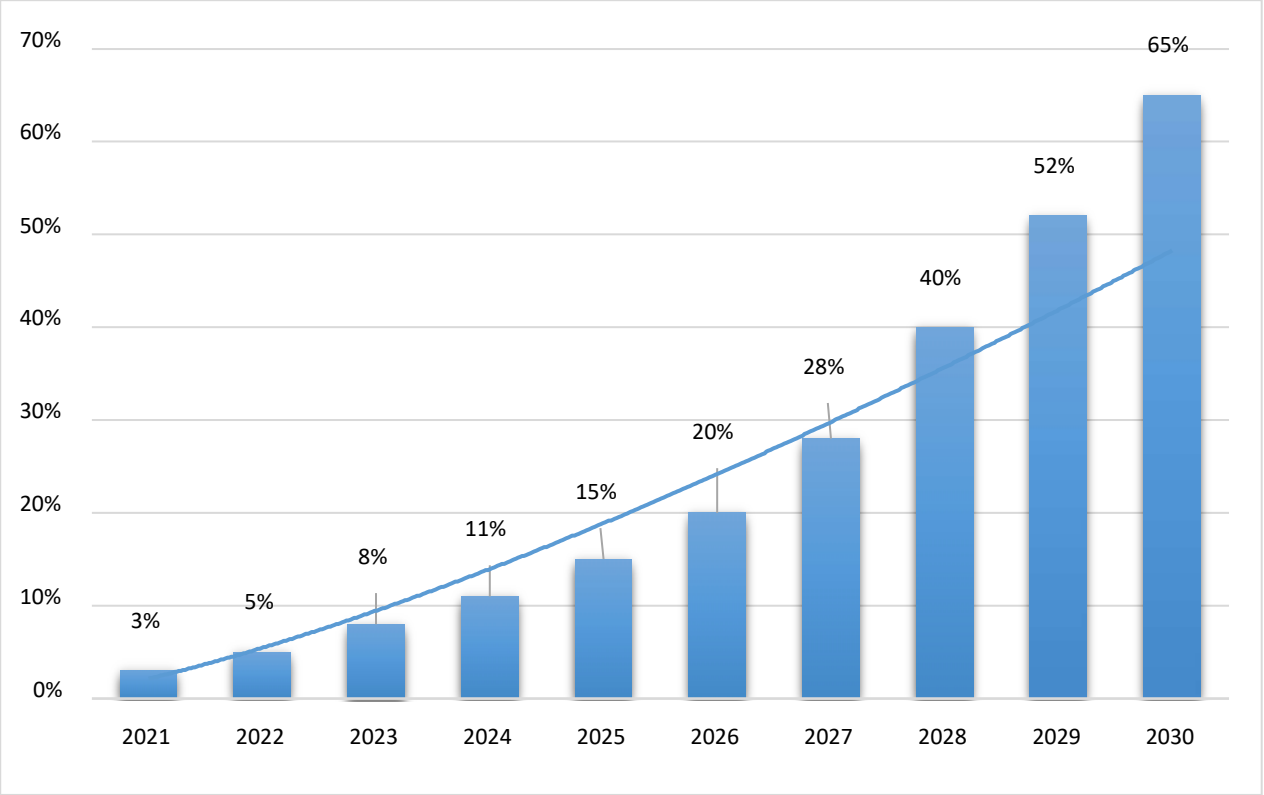


Рис. 3.1. Впровадження цифрових технологій та їхній вплив на ВВП України до 2030 року

Примітка. Джерело: [3]

Процес цифровізації важливий для української економіки, оскільки може створити нові робочі місця та збільшити річний ВВП. Створення нових ринків і галузей сприятиме зростанню підприємств і галузей. Крім того, дослідники прогнозують, що ринок праці створить додаткові 700 000 робочих місць, якщо нові інновації будуть включені в усі сфери економіки. Фінансування оцифрування розподіляється між внутрішнім і міжнародним ринками. Інвестиції в цифровізацію бізнесу, виробництва та промисловості оцінюються в мільярди доларів.

Сьогодні, в умовах сталого розвитку, в Україні сформовано Стратегію сталого розвитку України до 2030 року [42] та Національний план дій до 2020

року. Ці документи розроблено українськими професіоналами та експертами з метою посилення та прискорення сталого розвитку України.

Обидва документи покликані виконувати функцію важеля для реалізації основ розвитку всієї країни та регіону. За умови їх затвердження на державному рівні ця мета може бути досягнута. Основою Стратегії сталого розвитку є довгострокові стратегічні орієнтири сталого розвитку України. Врахування досвіду ЄС має вирішальне значення для екологічної політики українського уряду.

Стратегія сталого розвитку є наймасштабнішим національним документом планування розвитку. Він визначає основні цілі держави та суспільства для досягнення збалансованого та сталого розвитку.

Стратегія сталого розвитку України (рис. 3.2) складається із семи стратегічних завдань.

Рис.3.2. Основні аспекти Стратегії сталого розвитку України до 2030 р.

Примітка. Джерело: узагальнено на основі [42]

Досліджуючи Стратегію сталого розвитку до 2030 року [42], автор може зробити висновок, що цифровізація сприймається урядом України як засіб національного розвитку. В Україні вже створено необхідні основи для успішного цифрового уряду.

Технології оцифрування сприяють полегшенню доступу до культури, збереженню мови та культури України, сприяють розвитку національної ідентичності країни. У рамках дослідження автор запропонував першу мету цифрової економіки – створення цифрового культурного простору.

Наступним пріоритетом, як він пропонує, є цифрові інвестиції в людський капітал. Надання постійної освіти та цифрового контенту, який сприяє інвестиціям у цифрову економіку.

Автор вважає, що оцифрування відіграє роль у зміні освітньої парадигми шляхом підвищення доступності цифрових ресурсів, оцифрування шкіл, бібліотек і навчальних матеріалів, а також електронного навчання. Як наслідок, пріоритет 3 – цифровізація освіти.

За допомогою відкритих знань і наукових зусиль, віртуальних бізнес-інкубаторів, цифрових мереж і платформ можна розвинути інноваційну та екологічно ефективну цифрову економіку – пріоритет № 4. Цифрове відтворення прав власності дозволить отримати доступ до інтелектуальної власності та знизити вартість відтворення . Перехід від транспорту до дистанційної зайнятості та дистанційної освіти також негативно вплине на споживання енергії та викиди вуглецю.

Наступним пріоритетом, як вказує автор, є визначення природних ресурсів, які можуть бути використані для генерування капіталу в майбутньому. За допомогою цифрових технологій та платформ будуть популяризуватися та впроваджуватися нові методи зменшення впливу людської діяльності на навколишнє середовище.

Впровадження високошвидкісних широкосмугових мереж сприятиме сучасному наданню цифрових послуг у сільській та віддалених районах, що сприятиме регіональному розвитку (пріоритет 6).

Зрештою, цифровізація вважається засобом підвищення суспільних інновацій та участі (пріоритет 7). Електронне врядування може надавати ефективніші послуги більш ефективним чином, соціальні мережі та онлайн-платформи можуть служити форумом для громадян, щоб обмінюватися ідеями та співпрацювати у вирішенні соціальних проблем.

Збереження цих пріоритетів можливе в контексті певних дій і вдосконалень. Пріоритет 1 може бути досягнутий шляхом впровадження системи управління людськими ресурсами в державному управлінні, яка базується на електронному урядуванні. Досягнення цієї мети можливе через створення бази даних досліджень і публікацій українських учених, письменників, науковців та відтворення української культурної спадщини.

Створення та підтримка мережі експертів у сфері цифрової культури також сприятиме роботі пріоритету. Підвищуючи здібності працівників і підприємців до електронних навичок, інформаційної грамотності та алгоритмічного мислення, це гарантуватиме реалізацію пріоритету номер два.

Пріоритет 3 буде вирішено шляхом створення цифрових навчальних матеріалів. Ергономічний дизайн планування школи та інноваційні рішення щодо ІКТ у регіональних школах та підготовка вчителів, у тому числі у сфері ІКТ, також сприятимуть пріоритету 3.

Інноваційна та екологічно ефективна економіка (пріоритет 4), що забезпечує об’єднання існуючої інфраструктури електронних комунікацій та створення комплексної бази даних щодо зміни клімату та якості повітря. Підтримка нових продуктів і технологій сприятиме досягненню пріоритетної мети.

Природні активи, пов’язані з капіталом майбутнього (Пріоритет 5), можна досягти шляхом вивчення способів пом’якшення зміни клімату та створення порталу щодо зміни клімату та інформаційної системи щодо зон ризику повеней, а також шляхом проведення оцінки існуючих електронних комунікаційних мереж. Це сприятиме регіональному розвитку (пріоритет 6).

Збільшення інновацій та участі громадськості (пріоритет 7) буде досягнуто шляхом створення централізованих ІКТ-платформ, призначених для державного управління та оцифрування державних послуг. Використання системи прогнозування ринку праці та взаємодія з цивільним населенням у Web 2.0 гарантує участь громадськості в цифровій економіці. Електронні послуги та системи, пов'язані із законом, а також підвищення обізнаності громадськості щодо безпеки персональних даних сприяють зростанню урядових інновацій. Інформування державних органів про необхідність забезпечення безпеки обробки персональних даних в мережі Інтернет та забезпечення високого ступеня захисту дій з персональними даними гарантуватиме досягнення пріоритету 7.

Розробляючи стратегію розвитку цифрової економіки, на думку автора, важливо звернути увагу на способи комунікації влади з громадськістю. Потрібні три кроки, щоб зробити уряд більш відданим розвитку цифрової економіки.

Перший крок – «Політична цифрова трансформація». Метою якого є сприяння цифровій трансформації політики більшою мірою в політичному житті держави. Мета цифрової трансформації має бути включена до Стратегії сталого розвитку та Національного плану розвитку. У цих документах бракує інформації щодо характеру чи масштабу цифрової трансформації. Підвищення важливості політики цифрової трансформації сприятиме розвитку цифрової економіки. Існує необхідність надати доступ до можливостей для перегляду стратегії, щоб забезпечити більш потужну та більш віддану прихильність цифровій трансформації.

Другий крок, яким є «Інвестиції для інформаційного суспільства», поєднує планування фінансування та сприяння інвестиційній діяльності, яка призведе до швидшого розвитку інформаційного суспільства. Доцільно делегітимізувати виконання цих правил кожному департаменту, кожен департамент матиме більш повне розуміння своєї сфери відповідальності, але існує необхідність створити більш конкретні бюджетні асигнування та виділити більше грошей до бюджету департаменту. Це сприятиме підвищенню прозорості та ефективності витрат.

Наступним і останнім кроком є встановлення «інституціоналізованих механізмів», які сприятимуть цифровій трансформації уряду. Відсутність формального національного підходу до цифрової трансформації знижує загальну ефективність програми цифрової трансформації України. Стратегія базується на заклику до збалансованої інтеграції цифровізації в галузеву політику з достатніми ресурсами для координації політики, відповідним фінансуванням і амбітними, але реалістичними цілями.

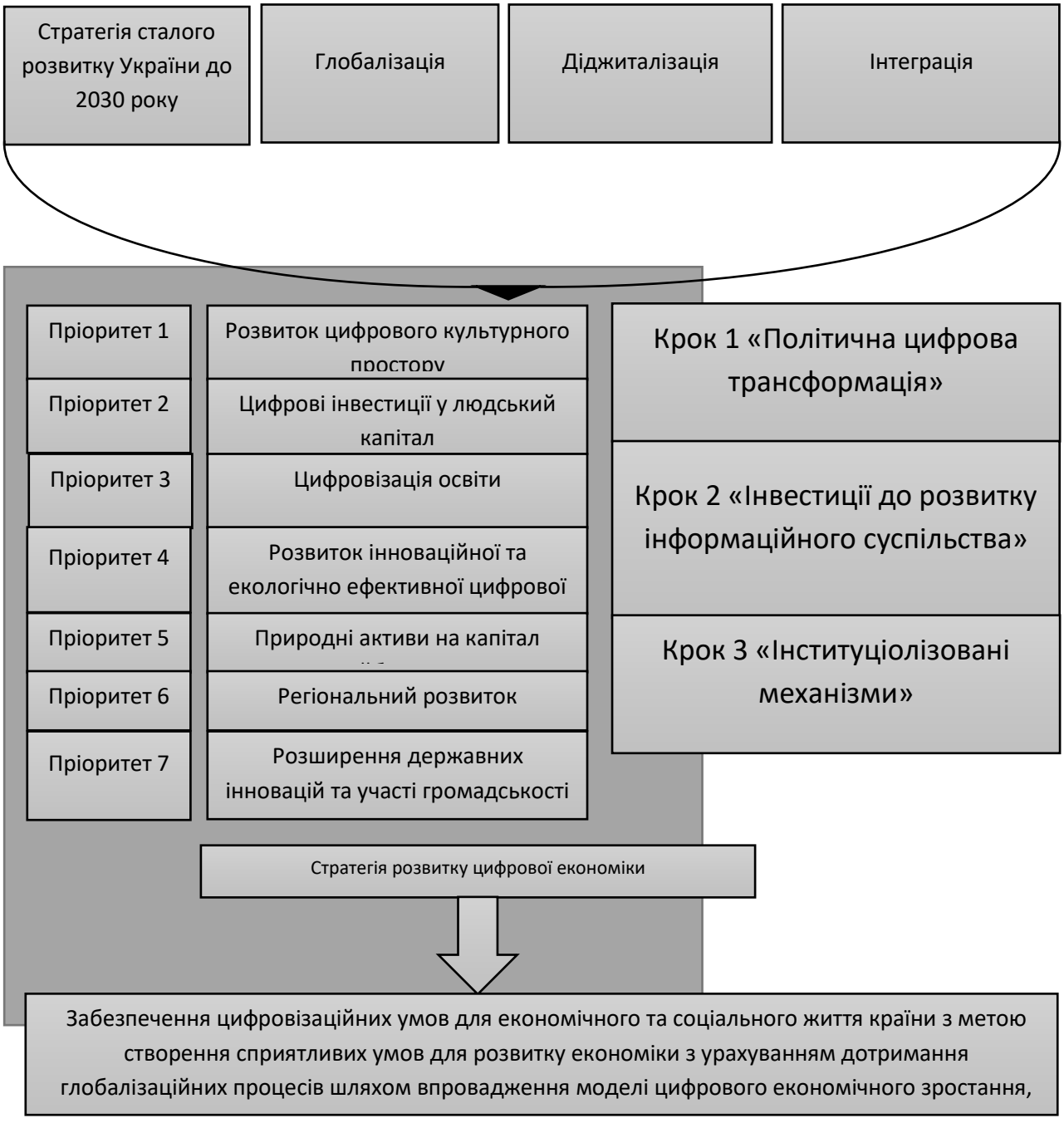


Рис. 3.3. Ключові складові стратегії розвитку цифрової економіки

Примітка. Джерело: узагальнено на основі [42]

Деякі країни мають спеціальне міністерство чи орган, який опікується національною цифровою стратегією, тоді як інші мають портфель координації національної цифрової стратегії для конкретного міністра чи органу. У деяких випадках координація делегується кільком установам або здійснюється на найвищому рівні уряду.

Незважаючи на унікальні особливості, переваги та недоліки кожної країни, вкрай важливо, щоб Україна, враховуючи попередній досвід, могла сприяти координації їхніх цифрових стратегій. Автор вважає, що цього можна досягти політичними засобами та ресурсами, які допоможуть уряду в розвитку цифрової економіки.

Як наслідок, прихильність уряду до розвитку цифрової економіки через реалізацію Стратегії розвитку цифрової економіки сприятиме довгостроковому розвитку України. Використання цифрових технологій для підвищення якості життя та умов ведення бізнесу призведе до нових можливостей як для населення, так і для уряду.

Загалом, кібербезпека стала однією з головних загроз для національної безпеки України в умовах війни. Інформаційні та кібератаки, що ведуться з боку ворога, ставлять під загрозу інфраструктуру, економіку та державні інститути країни. За даними Державної служби спеціального зв'язку та захисту інформації України, кількість кібератак значно зросла після початку російської агресії у 2014 році та повномасштабного вторгнення у 2022 році [81].

Отже, для забезпечення стійкості України у військовий, враховуючи окреслені пріоритетні напрями розвитку інфораструктури протидії кіберзагрозам, необхідно акцентувати увагу на наступних завданнях в рамках наявної Стратегії кібербезпеки України (рис. 3.4).

Одним із ключових елементів удосконалення стратегії кібербезпеки є розвиток інституційної спроможності державних органів, відповідальних за кіберзахист. Важливо, щоб національні та військові структури, зокрема Державна служба спеціального зв'язку, Національний координаційний центр кібербезпеки та Збройні сили України, діяли скоординовано та в режимі

реального часу. Створення національного кіберопераційного центру, який об’єднував би різні структури, відповідальні за кібербезпеку, і забезпечував координацію дій під час кібератак, дозволив би оперативно реагувати на загрози та запобігати критичним наслідкам для держави.

Рис. 3.4. Приорітетні завдання в рамках наявної Стратегії кібербезпеки України

Примітка. Джерело: розроблено автором

Оскільки велика частина критичної інфраструктури перебуває у приватних руках, важливо впровадити механізми обміну інформацією та швидкої взаємодії для захисту ключових об'єктів. Тому важливо зміцнити співпрацю між приватним сектором і державними установами.

Критична інфраструктура — один із основних об'єктів атак під час війни. Під загрозою можуть бути енергетичні системи, транспортні вузли, фінансові мережі та комунікації. Одним із пріоритетів є підвищення захищеності критичних систем через впровадження сучасних технологій захисту. Це включає в себе системи раннього виявлення кібератак, інструменти моніторингу мереж, а також впровадження автоматизованих рішень для відновлення роботи після атаки. Актуальним є розширення кіберрезервів та спеціалізованих кіберсил у

структурі Збройних сил України для захисту від військових кіберзагроз. Успішні приклади таких структур можна спостерігати в країнах НАТО, де кіберзахист інтегрований у загальну оборонну стратегію.

Для успішного протистояння кібератакам необхідно забезпечити високий рівень підготовки фахівців у галузі кібербезпеки. Україна повинна інвестувати в розвиток освітніх програм у вищих навчальних закладах та спеціалізованих тренінгів для фахівців різних рівнів. Запровадження масштабних освітні програми з кібербезпеки для державних службовців та військових дозволить ефективно реагувати на кіберзагрози. Підтримка академічних та науково-дослідних ініціатив у сфері кіберзахисту для розвитку нових технологій та рішень, можуть бути інтегровані в державну стратегію.

Україна має активно розвивати міжнародну співпрацю у сфері кібербезпеки. Це дозволить отримати доступ до нових технологій, інформації про загрози, а також підтримку від союзників. Активізація співпраці з НАТО та ЄС для інтеграції України у міжнародні кіберсистеми та обміну даними про загрози, окрім технічної підтримки, дасть змогу брати участь у спільних кібернавчаннях, що покращить готовність до відбиття атак. Підписання міжнародних угод про кібербезпеку для обміну даними про загрози та спільної розробки стандартів кіберзахисту забезпечить стабільність співпраці в майбутньому.

Україна має впроваджувати передові технології для захисту своїх інформаційних ресурсів. У цьому контексті важливо використовувати штучний інтелект та машинне навчання для автоматизованого виявлення аномалій у кіберпросторі. Це дозволить швидко ідентифікувати та реагувати на потенційні загрози. Блокчейн-технології можуть бути використані для захисту урядових баз даних та важливої інформації від несанкціонованих втручань, оскільки вони забезпечують високу прозорість та неможливість змін даних без дозволу.

Отже, в умовах військового стану удосконалення стратегії кібербезпеки України є надзвичайно важливим для захисту національної безпеки та критичної інфраструктури. Посилення інституційної спроможності, модернізація

критичних систем, міжнародна співпраця та впровадження нових технологій є ключовими елементами, що дозволять Україні протистояти кіберзагрозам в сучасному світі. Кібербезпека повинна бути інтегрованою частиною національної стратегії оборони, а держава повинна інвестувати в підготовку кадрів і розвиток кіберінфраструктури для ефективного протистояння новим викликам.

3.2 Напрями удосконалення стратегії кібербезпеки України як гарантії національної безпеки

На сьогодні неминучим стало впровадження штучного інтелекту і роботів в економіку, виробництво, освіту, науку, охорону здоров'я та інші сфери життєдіяльності. Людина як об'єкт, що впливає на перебіг виробничого циклу, замінюється програмами, які визначають за цифровими алгоритмами спосіб мислення штучного інтелекту і поведінку роботів.

Цифрові технології стали невід'ємною частиною сучасного життя майже кожної людини. Так, понад 60% населення планети підключені до Інтернету, користуються цифровими технологіями, отже, не можна недооцінювати їхній вплив на суспільство [71-76].

З огляду на останні події, пов'язані з популяризацією технології штучного інтелекту, з упровадженням технологій у побут, у повсякденність більш ніж кожної другої людини на планеті; і обиватели, і експертне співтовариство обговорюють питання практик і меж використання обговорюваних результатів людської діяльності. Особливо це питання актуальне для формування стратегії цифрової трансформації економіки і стратегії кібербезпеки України.

Змагання за світове лідерство в галузі штучного інтелекту розпочато. За 2024 рік місяців Канада, Японія, Сінгапур, Китай, ОАЕ, Фінляндія, Данія, Франція, Велика Британія, Комісія ЄС, Південна Корея та Індія реалізували стратегії, що спрямовані на сприяння розвитку AI. Немає двох однакових стратегій, кожна зосереджена на різних аспектах AI, зокрема, на таких як наукові

дослідження, розвиток талантів і навичок, навчання, адаптація державного та приватного секторів, етика та інклюзія, створення стандартів та нормативних вимог, а також дані та цифрова інфраструктура.

Загальні тенденції використання технологій ШІ в світі вражають стрімкими темпами розвитку (рис. 3.5.). За оцінками Statista [89] до 2050 року, світовий обсяг цього ринку сягне 826,73 більонів долларів США.

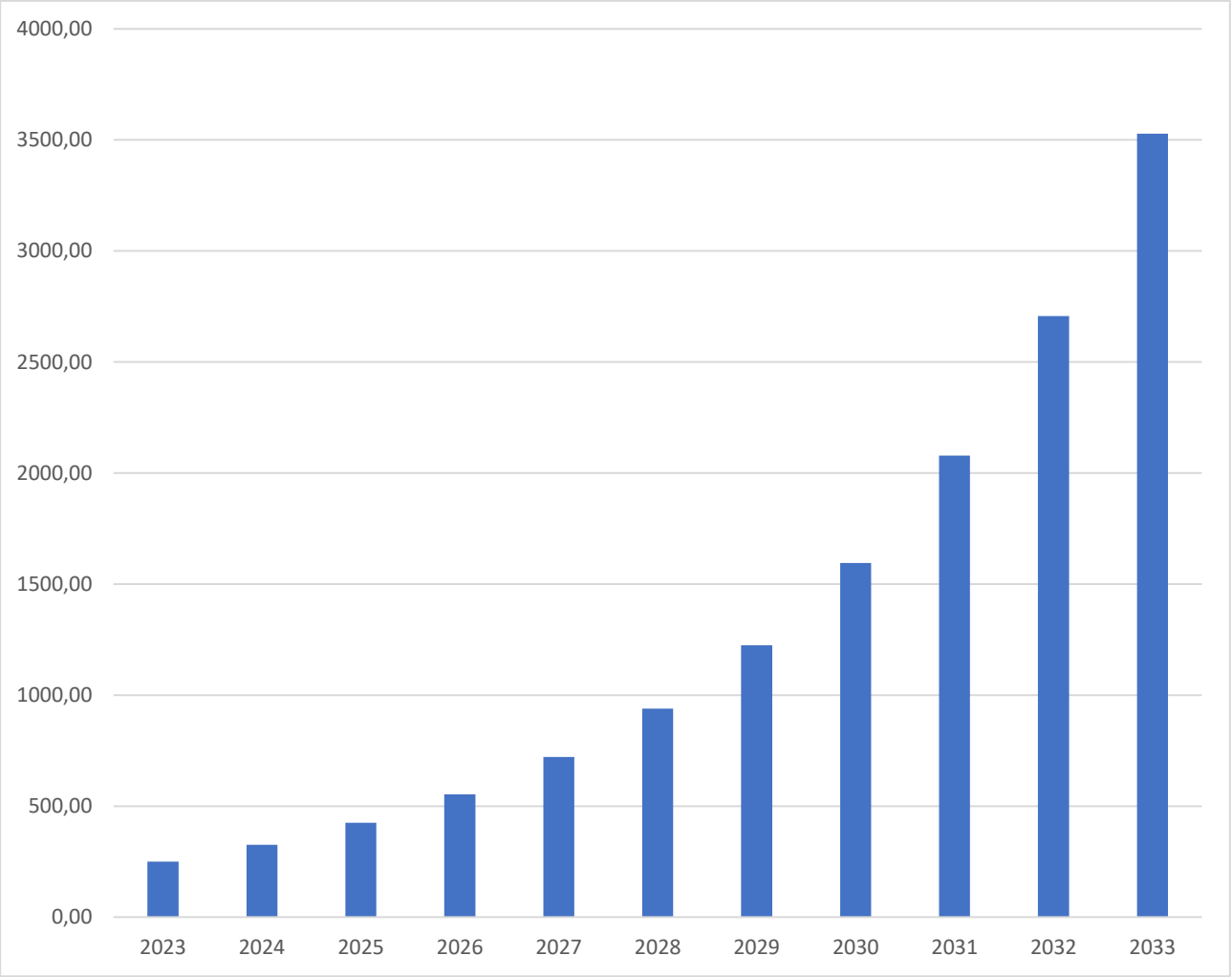


Рис. 3.5. Глобальний ринок штучного інтелекту, 2023–2033 рр., млрд дол. США

Примітка. Джерело: [89]

У період з 2020 по 2022 рік щорічні корпоративні інвестиції в стартапи зі штучним інтелектом зросли до п’яти мільярдів доларів США. Майже втричі більше, ніж попередні інвестиції, причому значна частина їх – приватні інвестиції американських компаній.

Найновіші високоякісні компанії штучного інтелекту включають усі компанії, що займаються чат-ботами та машинним навчанням, які зосереджені на інтерфейсах людини та машини.

Аналогічні тенденції зростання можна прослідкувати по кількості користувачів інструментів штучного інтелекту (AI) у всьому світі (рис. 3.6).

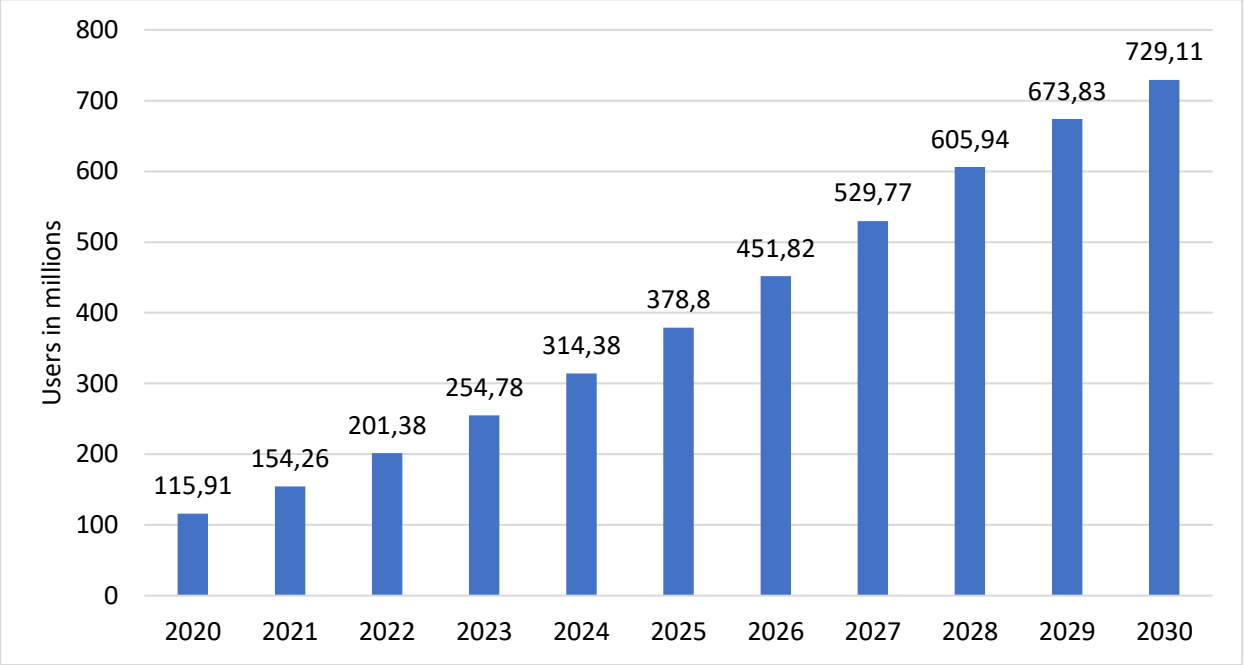


Рис. 3.6. Кількість користувачів інструментів штучного інтелекту (AI) у всьому світі з 2020 по 2030 рік (в мільйонах)

Примітка. Джерело: [89]

Прогнозується, що глобальна кількість користувачів інструментів штучного інтелекту в сегменті «Користувачі інструментів штучного інтелекту» на ринку буде постійно зростати між 2024 і 2030 роками загалом на 414,7 мільйонів (+131,91 відсотка). Після десятого року поспіль кількість користувачів інструментів штучного інтелекту, за оцінками, складе 729,11 мільйонів, а отже, досягне нового піку в 2030 році.

Світовий рівень зростання кількості користувачів інструментів штучного інтелекту показує загальні тенденції. Але, в різних країнах світу ситуація різниця. Глобальний індекс AI 2024 підкреслює, що уряди в усьому світі починають розглядати AI як стратегічний пріоритет. Завдяки потужним

екосистемам штучного інтелекту та підтримці уряду інші країни досягають величезного прогресу, навіть якщо США та Китай все ще займають домінуючу позицію. Потенціал країн покращити свій потенціал штучного інтелекту шляхом цілеспрямованих інвестицій у персонал, дослідження та інфраструктуру демонструє приголомшливий підйом Франції та послідовне зростання Німеччини.

Країни ранжуються за їхнім потенціалом ШІ на міжнародному рівні. П'ята ітерація Global AI Index, опублікована 19 вересня 2024 року демонструє позиції країн за напрямами (табл. 3.2).

Таблиця 3.2

Вибірковий рейтинг країн за глобальним індексом AI 2024

Rank	Country	Talent	Infra-structure	Operating Environ-ment	Research	Deve-lopment	Govern-ment Strategy	Com-mercial
1	United States	1	1	2	1	1	2	1
2	China	9	2	21	2	2	5	2
3	Singapore	6	3	48	3	5	10	4
4	United Kingdom	4	17	4	4	16	7	5
5	France	10	14	19	6	4	9	8
6	South Korea	13	6	35	13	3	4	12
7	Germany	3	13	8	8	11	8	9
8	Canada	8	18	19	9	10	3	6
9	Israel	7	26	65	7	6	32	3
10	India	2	68	3	14	13	11	13
55	Ukraine	51	59	38	65	48	40	60

Примітка. Джерело: [100]

Категорія «Талант» зосереджується на наявності кваліфікованих практиків у сфері рішень штучного інтелекту. Категорія «Інфраструктура» оцінює надійність і масштаб інфраструктури доступу, від електроенергії та Інтернету до можливостей суперкомп'ютера. «Робоче середовище» фокусується на нормативному контексті та громадській думці щодо штучного інтелекту.

Категорія «Дослідження» розглядає обсяг спеціалізованих досліджень і дослідників, включаючи кількість публікацій і цитування в надійних

академічних журналах. «Розробка» зосереджена на розробці фундаментальних платформ і алгоритмів, на яких спираються інноваційні проекти штучного інтелекту. «Урядова стратегія» вимірює глибину прихильності національних урядів штучному інтелекту; дослідження зобов'язань щодо витрат і національних стратегій. Категорія «Комерціалізація» фокусується на рівні активності стартапів, інвестицій та бізнес-ініціатив на основі штучного інтелекту.

Як видно з табл. 3.2, Україна займає 55 позицію. Лідируючи позиції займають США, Китай, Сінгапур. По категоріям аналізу можна відзначити значний вплив наукової складової на результати рейтингу. Отже, зазначені тенденції свідчать не тільки про стрімке зростання користувачів технологіями ШІ, а й про нагальну необхідність забезпечення цифрових навичок в суспільстві і свідомого використання технологій ШІ в освіті.

Аналіз стратегії кібербезпеки України показав, що серед 94 завдань та індикаторів виконання стратегії кібербезпеки України тільки 1 в переліку окреслює заходи з протидії кіберзлочинності в сфері штучного інтелекту. До кінця другого півріччя 2022 року розроблено (створено концептуальне бачення, затверджено необхідні нормативно-правові документи та проведено пілотне застосування) механізму стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням розвитку новітніх інформаційно-комунікаційних технологій.

Щорічно механізм забезпечує стимулювання мінімум одного нового дослідження чи розробки в наступних категоріях: технології хмарних та квантових обчислень, 5G-мережі, Інтернет речей, штучний інтелект, нові засоби реалізації кіберзагроз, створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки.

Щорічно до НКЦК подається довідкова інформація про результативність застосування механізму.

З огляду на темпи використання технологій штучного інтелекту в суспільстві, варто стимулювати інновації щодо протидії кіберзлочинності в сфері штучного інтелекту. Тому пропонуються напрями подальшого

удосконалення стратегії кібербезпеки України з огляду на стрімкий розвиток технологій штучного інтелекту та індикаторів її виконання.

Стрімкий розвиток технологій штучного інтелекту (ШІ) відкриває нові можливості для підвищення ефективності різних галузей, але також несе нові виклики для сфери кібербезпеки. З огляду на агресію з боку Росії та постійні кіберзагрози, Україна повинна адаптувати свою стратегію кібербезпеки до сучасних умов. Інтеграція ШІ в національну стратегію кібербезпеки може значно підвищити ефективність протидії загрозам, але також вимагає нових підходів до захисту від технологічних ризиків, пов'язаних із самим штучним інтелектом (рис. 3.7).

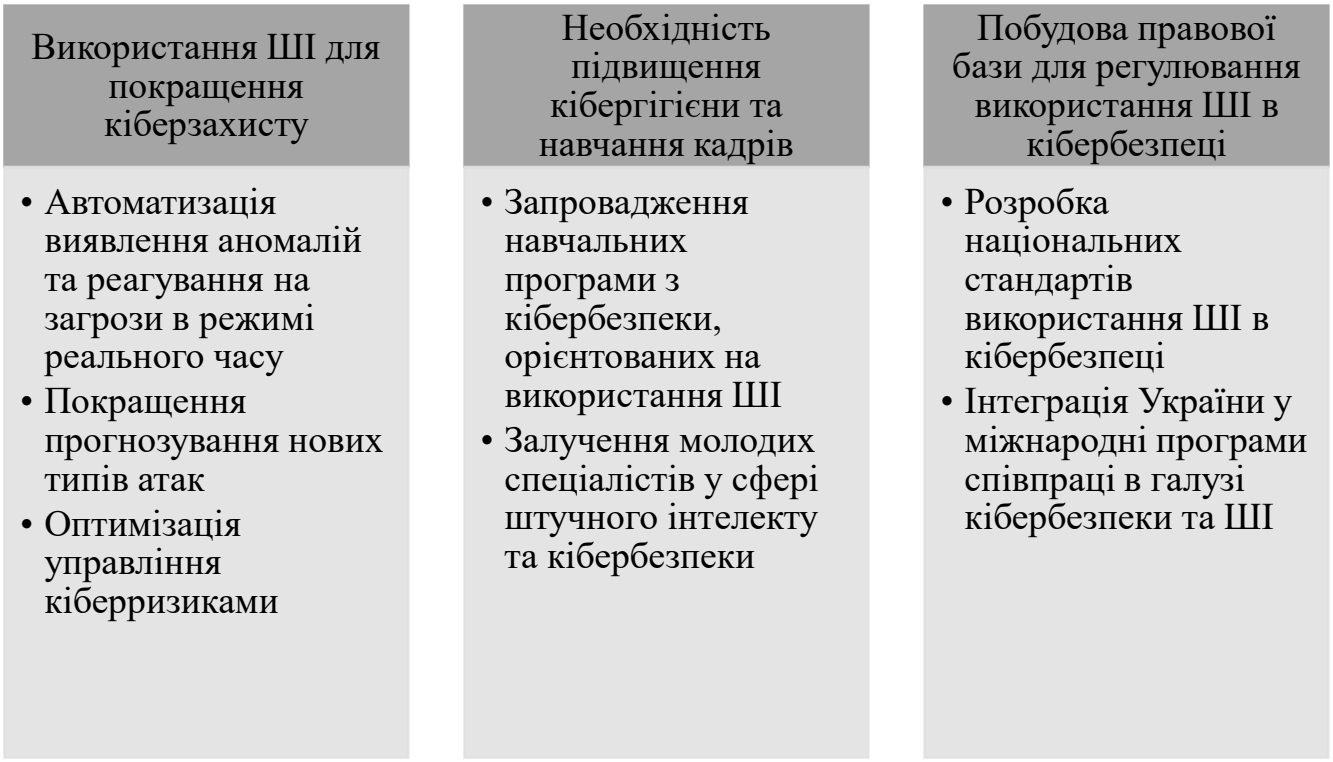


Рис. 3.7 Напрями розвитку стратегії кібербезпеки України

Примітка. Джерело: розроблено автором

Штучний інтелект відкриває широкі можливості для автоматизації процесів виявлення та протидії кібератакам. Алгоритми машинного навчання можуть аналізувати величезні обсяги даних і виявляти аномалії, які можуть бути ранніми ознаками загроз. ШІ може допомогти автоматизувати виявлення аномалій та реагування на загрози в режимі реального часу. Наприклад, компанія IBM зазначає, що використання ШІ в кібербезпеці допомагає скорочувати час реагування на загрози і підвищує ефективність аналізу подій безпеки [91-92]. Покращення прогнозування нових типів атак за допомогою систем прогнозного аналізу дозволить ефективніше реагувати на загрози до того, як вони досягнуть критичних систем. Оптимізація управління кіберризиками, завдяки аналізу величезної кількості метаданих і побудові моделей кіберзахисту, дозволить враховувати потенційні вразливості.

Разом із перевагами, які ШІ може принести для кіберзахисту, він також може використовуватися зловмисниками для підвищення ефективності кібератак. Одним з основних ризиків є автоматизація та персоналізація атак. ШІ може бути використаний для:

- Фішингових атак, що адаптуються до кожного конкретного користувача, створюючи більш переконливі та складні для виявлення шкідливі повідомлення. За даними аналітиків компанії Palo Alto Networks, розвиток ШІ значно підвищив ефективність фішингових кампаній завдяки можливості генерації персоналізованих контентів [94];
- Атаки на штучний інтелект (адверсаріальні атаки), коли зловмисники змінюють дані, які використовуються ШІ для навчання, що може призвести до помилкових висновків та порушення роботи захисних систем. Це становить особливу загрозу для державних структур та критичної інфраструктури.

Щоб ефективно використовувати штучний інтелект у стратегії кібербезпеки, необхідно значно підвищити рівень кібергігієни серед державних службовців та бізнесу. Україна вже активно працює в цьому напрямку, але через динаміку розвитку ШІ слід впроваджувати нові освітні програми, що охоплюють основи роботи зі штучним інтелектом. Запровадження навчальних програм з

кібербезпеки, орієнтованих на використання ШІ для державних установ, армії та підприємств критичної інфраструктури. Це сприятиме не лише підвищенню рівня знань, але й зменшенню людських помилок, які часто є причиною успішних кібератак. Залучення молодих спеціалістів у сфері штучного інтелекту та кібербезпеки до роботи в державних структурах дасть змогу інтегрувати інновації швидше та більш ефективно.

Для забезпечення кібербезпеки та ефективного використання ШІ важливо розробити відповідну правову базу. ШІ може впливати на безпеку не лише через атаки, але й через неконтрольоване використання технологій у критично важливих системах. Розробка національних стандартів використання ШІ в кібербезпеці дасть змогу регулювати впровадження та використання ШІ, встановлюючи рамки відповідальності та захисту персональних даних. Інтеграція України у міжнародні програми співпраці в галузі кібербезпеки та ШІ дозволить розширити можливості отримання інформації про новітні технології захисту, обміну досвідом та інноваціями.

Україна вже є активним учасником міжнародних ініціатив у галузі кібербезпеки, зокрема в рамках співпраці з НАТО та ЄС. Однак розвиток технологій штучного інтелекту вимагає розширення такої співпраці. Україна має розширювати кібердипломатію через обмін досвідом із партнерами по НАТО, оскільки багато країн Альянсу вже інтегрують ШІ у свої оборонні стратегії [93-95] та співпрацювати з міжнародними технологічними компаніями, що займаються розробкою ШІ. Такі компанії можуть надавати Україні інноваційні рішення та брати участь у розвитку захисних систем.

Інтеграція штучного інтелекту у стратегію кібербезпеки України є важливим кроком для підвищення ефективності захисту в умовах сучасних загроз. Використання ШІ може значно покращити виявлення та реагування на кіберзагрози, але водночас вимагає підвищення уваги до нових ризиків, які виникають через розвиток цієї технології. Для успішного впровадження ШІ у кібербезпеку необхідно підвищити рівень кіберосвіти, адаптувати правову базу та розширювати міжнародну співпрацю в цій сфері.

Висновки до розділу 3

Відданість уряду розвитку цифрової економіки сприятиме довгостроковому розвитку України. Використання цифрових технологій для підвищення якості життя та умов ведення бізнесу призведе до нових можливостей як для населення, так і для уряду.

Для забезпечення військової стабільності країни, враховуючи окреслені принципи пріоритетності розвитку інформаційної інфраструктури країни для протидії кіберзагрозам, необхідно зосередити увагу на наступних завданнях у рамках діючої Стратегії кібербезпеки України. Україна має використовувати передові технології для захисту своїх інформаційних ресурсів. У цьому контексті вкрай важливо використовувати штучний інтелект і машинне навчання для автоматичного виявлення збоїв у кіберпросторі. Це сприятиме швидкому розпізнаванню та реагування на потенційну небезпеку. Технології блокчейн можна використовувати для захисту державних даних і важливої інформації від зловмисного вторгнення, оскільки вони забезпечують високий ступінь прозорості та неможливість змінювати дані без авторизації.

Щоб забезпечити безпеку свого кібер-життя та ефективне використання штучного інтелекту, ви повинні створити правову базу. Штучний інтелект може негативно вплинути на безпеку, окрім самих атак, можливе також ненавмисне використання технологій у критично важливих системах, які мають місію. Створення національних стандартів щодо використання ШІ в кібербезпеці сприятиме регулюванню того, як і чому ШІ використовується в кібербезпеці, а також захисту персональних даних. Інтеграція України в міжнародні програми, присвячені кібербезпеці та ШІ, сприятиме отриманню інформації щодо найновіших засобів захисту, обміну досвідом та інноваціями.

Швидка еволюція технологій штучного інтелекту привела до нових можливостей у різних галузях, але також поставила нові виклики для сфери кібербезпеки. Враховуючи схильність Росії до агресії та постійні загрози в кіберпросторі, Україна повинна змінити стратегію безпеки в кіберсфері з

урахуванням сучасних обставин. Інтеграція штучного інтелекту в національну стратегію кібербезпеки може значно вплинути на ефективність протидії загрозам, однак це також вимагає нового підходу до боротьби з технологічними небезпеками, пов’язаними з самим ШІ.

ВИСНОВКИ

Розвиток цифрових технологій слід розглядати як використання та впровадження цифрових технологій у всі сфери життя, результатом чого є створення інноваційних продуктів, послуг і рішень, які підвищують ефективність, продуктивність і конкурентоспроможність у різних галузях. Він сприяє використанню обчислювальних і цифрових методів для створення нових технологій, платформ і систем, які вирішують проблеми користувачів і практичні для суспільства.

Характеристики стратегій міжнародного бізнесу щодо цифрової трансформації в контексті «Суспільства 5.0» очевидні:

1. Глобальний масштаб: у контексті «Суспільства 5.0» цифрова трансформація тепер є глобальним явищем, яке охоплює не лише окремі країни, а й увесь світовий ринок. Міжнародні стратегії спрямовані на вихід на різні ринки, формування партнерства по всьому світу та використання міжнародних ресурсів.

2. Культура різноманітності: міжнародні стратегії повинні враховувати культурні відмінності між країнами, з якими компанія взаємодіє. Розуміння культурних відмінностей і вміння адаптуватися допомагає зберегти значну перевагу та збільшити успіх цифрових стратегій.

3. Технологічні інновації: Суспільство 5.0 характеризується використанням передових технологій, таких як штучний інтелект, Інтернет речей, блокчейн тощо. Міжнародні стратегії мають сприяти впровадженню цих інновацій і створенню нових цифрових рішень, які підходять для кожного ринку.

4. Глобальна конкуренція: природа «Суспільства 5.0» створює нові можливості для глобальної конкуренції. Міжнародні стратегії повинні враховувати конкурентний характер ринків у різних країнах і розробляти стратегії, які мають перевагу.

5. Партнерство та співпраця: міжнародні стратегії в контексті «Суспільства 5.0» спрямовані на формування партнерства та співпраці з іншими корпораціями,

установами та країнами. Поєднання ресурсів, здібностей та інноваційних знань позитивно впливає на реалізацію цифрових проектів на міжнародному рівні.

Ці атрибути визначають необхідність розробки всебічних і універсальних міжнародних стратегій цифрової трансформації, які враховують унікальні характеристики кожного ринку, позитивно впливають на глобальну конкурентоспроможність і призводять до сталого та інноваційного бізнесу в контексті «Суспільства 5.0».

Зараз Україна має скромний потенціал для просування цифрової трансформації. Проте вкрай важливо визнати, що ці можливості супроводжуються викликами, які вимагають державного регулювання для ефективного реагування. Створення інформаційно-комунікаційних технологій, програмного забезпечення та відповідної інфраструктури сприяє розвитку політики цифрової держави, яка ґрунтується на комплексному підході до вирішення проблем та обходу перешкод, усе це розглядається в контексті найкращих світових практик. Проте для успішної реалізації цієї політики необхідно створити ефективні механізми для кожного напряму, що є напрямком для майбутніх досліджень.

Під час дослідження було виявлено спільні риси та відмінності між регіонами світу. Між 2005 і 2022 роками кількість користувачів Інтернету значно зросла в усіх країнах світу, учетверо перевищивши поточну чисельність населення, з подальшим зростанням, яке очікується до 2025 року. Проте бідні країни мають у 3,5 рази менше шансів мати цей показник, ніж багаті країни.

Використання мобільного широкосмугового зв’язку в усьому світі зросло за останні кілька років, але країни з низьким рівнем доходу все ще відстають від країн з високим рівнем доходу з точки зору пропускної здатності мобільного зв’язку. Одним із найважливіших факторів доступу до бездротового Інтернету є наявність смартфона, вартість якого ускладнює адаптацію до цифрового світу в країнах з низьким рівнем доходу.

У всіх регіонах світу є мережі 4G, але менш розвинені країни значно відстають, вони все ще використовують 3G і 2G. І навпаки, покриття мережі 4G у містах більше, ніж у сільській місцевості в усіх регіонах.

Швидкість завантаження даних зростає як для фіксованої смуги пропускання, так і для мобільного зв'язку. Визначну роль у цьому відіграє наявність нової високошвидкісної інфраструктури передачі даних, через що розвинені країни часто поступаються прогресивним країнам, що розвиваються.

розвинені країни мають найкраще розуміння всіх аспектів Інтернет-бізнесу та послуг електронного уряду. В Азії найбільша кількість людей, які користуються соціальними мережами та шукають роботу в Інтернеті, тоді як в Африці найбільше людей, які завантажують програмне забезпечення. Азіатсько-Тихоокеанський регіон є найпопулярнішим споживачем міжнародної смуги пропускання.

Оцифровка каталізує швидке розширення цифрових платформ, і ці платформи матимуть різноманітне використання. Зростання цін на провідні процесори може означати зростання різниці між віртуальною та реальною економіками. Ланцюжок створення вартості даних зростає по всьому світу, і концепція національного суверенітету в цифровій економіці потребує подальшого уточнення. Майбутнє дослідження повинне вимірювати потоки даних, їх цінність і розрізняти необроблені дані та цифрові продукти.

У другому розділі досліджено методи науковців щодо визначення міжнародних метрик для вимірювання ступеня цифрового розвитку країн та визначено, які метрики оцінюють показники для України. Було детально розглянуто глобальний рейтинг цифрової конкурентоспроможності IMD, що дозволило не лише визначити позицію України в міжнародних рейтингах, а й оцінити субіндекси та субфактори процесу цифровізації в Україні. Ця інформація була використана для визначення переваг і недоліків процесу цифровізації в Україні. Отримані результати можуть бути використані при створенні стратегій зміни процесів у бізнесі, визначенні важливих напрямків, можливостей і перешкод, пов'язаних з інтеграцією цифрових технологій у діяльність компаній.

Результати нашого дослідження свідчать про те, що національна економіка поступово просувається до цифрової сфери, враховуючи європейську складову інтеграції. Навіть у поточному стані конфлікту Україна продовжує прагнення до цифрової трансформації та розвитку цифрової економіки. Робляться спроби створити умови для інноваційного бізнесу та забезпечити інституційну підтримку цих починань.

Швидкий розвиток технологій штучного інтелекту відкрив нові можливості для підвищення ефективності в різних галузях, але також створив нові виклики для сфери кібербезпеки. Враховуючи схильність Росії до агресії та постійні загрози в кіберпросторі, Україна повинна змінити стратегію безпеки в кіберсфері з урахуванням сучасних обставин. Інтеграція штучного інтелекту в національну стратегію безпеки кіберпростору може значно вплинути на ефективність протидії загрозам, однак це також вимагає нових методів захисту від потенційних небезпек, пов’язаних із самим ШІ. Щоб забезпечити безпеку свого кібер-життя та належне використання штучного інтелекту, ви повинні створити відповідний правовий клімат.

Штучний інтелект може негативно вплинути на безпеку, окрім самих атак, можливе також ненавмисне використання технологій у критично важливих системах, які мають місію. Створення національних стандартів щодо використання ШІ в кібербезпеці сприятиме регулюванню того, як і чому ШІ використовується в кібербезпеці, а також захисту персональних даних. Інтеграція України в міжнародні програми, присвячені кібербезпеці та ШІ, сприятиме отриманню інформації щодо найновіших засобів захисту, обміну досвідом та інноваціями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A Maturity Model for Digital Literacies and Sustainable Development / R.S.Sharma et al. *Encyclopedia of Information Science and Technology, Fourth Edition*. Hershey PA, USA, 2018. P. 2280–2291. DOI: https://doi.org/10.4018/ 978-1-5225-2255-3.ch198.

2. Digital Development – Plan International. *Plan International*. URL: https://plan-international.org/how-we-work/ digital-development-itc4d/.

3. Digital Development Compass. *UNDP Data Futures Platform*. URL: https://data.undp.org/digitalcompass/.

4. Digital Development. *World Bank*. URL: https://www.worldbank.org/en/topic/digitaldevelopment/overview.

5. Digital Strategy Development. *ICOM CIDOC*. URL: https://cidoc.mini.icom.museum/working-groups/digital- strategy-development/.

6. EU Digital Single Market. *EU4Digital*. URL: https://eufordigital.eu/discover-eu/eu-digital-single-market/.

7. Ghobakhloo M., Iranmanesh M. Digital transformation success under Industry 4.0: a strategic guideline for manufacturing SMEs. *Journal of Manufacturing Technology Management*. 2021. Ahead-of-print, ahead-of-print. DOI: https://doi.org/10.1108/jmtm-11-2020-0455.

8. Gorbul T., Rusakov S. Cultural Heritage in the Context of Digital Transformation Practices: Experience of Ukraine and the Baltic States. *Baltic Journal of Economic Studies*. 2022. Vol. 8, no. 4. P. 58–69. DOI: https://doi.org/ 10.30525/2256-0742/2022-8-4-58-69.

9. Hanna N. A role for the state in the digital age. *Journal of Innovation and Entrepreneurship*. 2018. Vol. 7, no. 1.DOI: https://doi.org/10.1186/s13731-018-0086-3.

10. Kim S., Choi B., Lew Y. K. Where Is the Age of Digitalization Heading? The Meaning, Characteristics, and Implications of Contemporary Digital Transformation. *Sustainability*. 2021. Vol. 13, no. 16. P. 8909. DOI: https://doi.

org/10.3390/su13168909.

11. Lucendo-Monedero A. L., Ruiz-Rodríguez F., González-Relaño R. Measuring the digital divide at regional level. A spatial analysis of the inequalities in digital development of households and individuals in Europe. *Telematics and Informatics*. 2019. Vol. 41. P. 197–217. DOI: https://doi.org/10.1016/j.tele.2019.05.002.

12. Oryshchuk V. Strategy as a mechanism for improving the state policy of digital development in the field of museum affairs. *Bulletin of Taras Shevchenko National University of Kyiv. Public Administration*. 2022. Vol. 16, no. 2. P. 28–35. DOI: https://doi.org/10.17721/2616-9193.2022/16-5/7.

13. Ostrovyj O. V. Backgrounds Of The Formation Of The State Digital Development Policy. *«Scientific Notes of Taurida V.I. Vernadsky University», series «Public Administration»*. 2021. No. 6. P. 37–43. DOI: https://doi.org/10.32838/ tnu-2663-6468/2021.6/06.

14. Peña-López I. Measuring digital development for policy-making: Models, stages, characteristics and causes: PhD Thesis. 29 p. URL: https://ictlogy.net/articles/20090908_ismael_pena-lopez_-_measuring_digital_development_ for_policy-making_(intro_conc).pdf.

15. Principles for Digital Development. *Principles for Digital Development*. URL: https://digitalprincip.wpengine. com/about/.

16. Søby M. Learning to Be: Developing and Understanding Digital Competence. *Nordic Journal of Digital Literacy*. 2013. Vol. 8, no. 03. P. 134–138. DOI: https://doi.org/10.18261/issn1891-943x-2013-03-01.

17. The Tracker Culture & Public Policy | Special Issue n 2 : Countdown to MONDIACULT 2022. *UNESCO*. URL: https://www.unesco.org/en/articles/tracker-culture-public-policy-special-issue-ndeg2-countdown-mondiacult-2022.

18. Деякі питання цифрового розвитку : Постанова Каб. Міністрів України від 30.01.2019 р. № 56 : станом на 5 берез. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/56-2019-п#Text.

19. Кожина А. Цифровий розвиток як пріоритетний напрям публічного

управління для стабілізації ситуації з наслідками пандемії COVID-19. *Збірник наукових праць Національної академії державного управління при Пре-зидентові України*. 2020. № 2. С. 134–140. DOI: https://doi.org/10.36030/2664-3618-2020-2-134-140.

20. Островий О. В. Формування державної політики цифрового розвитку: сучасні тенденції та перспекти- ви. *Таврійський науковий вісник. Серія: публічне управління та адміністрування*. 2022. № 3. С. 85–91. DOI: https:// doi.org/10.32851/tnv-pub.2021.3.12.

21. Подолання цифрового розриву в Україні: людиноцентричний підхід | United Nations development programme. *UNDP*. URL: https://www.undp.org/uk/ukraine/blog/подолання-цифрового-розриву-в-україні-людино- центричний-підхід

22. Про забезпечення реалізації деяких питань цифрового розвитку : Наказ Держ. агентства з питань елек- трон. урядування України від 09.04.2019 р. № 24. URL: https://zakon.rada.gov.ua/rada/show/v0024883-19#Text.

23. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та за- твердження плану заходів щодо її реалізації : Розпорядж. Каб. Міністрів України від 17.01.2018 р. № 67-р : станом на 17 верес. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-р#Text.

24. Про утворення Міжгалузевої ради з питань цифрового розвитку, цифрових трансформацій і цифровіза- ції : Постанова Каб. Міністрів України від 08.07.2020 р. № 595 : станом на 4 квіт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/595-2020-п#Text.

25. Свинарчук В. М. Prospects of society intellectualization in the context of the establishment of the Ministry of Digital Transformations of Ukraine. *Information and law*. 2020. № 4(35). С. 147–150. DOI: https://doi.org/10.37750/2616-6798.2020.4(35).221247.

26. Цифрові трансформації в Україні: чи відповідають вітчизняні інституційні умови зовнішнім викликам та європейському порядку денному?. *Поліс. фонд міжнар. та регіон. дослідж.,* 2020. 76 с. URL: http://eap-csf.org.ua/wp-

content/uploads/2021/04/Research_DT_PF_WG2_ua-1.pdf.

27. Дергачова Г.М., Колешня Я.О. Цифрова трансформація бізнесу: сутність, ознаки, вимоги та технології. *Еко-номічний вісник НТУУ «КПІ».* 2020. № 17. С. 280–290. DOI: https://doi.org/10.20535/2307-5651.17.2020.216367.

28. Суспільство 5.0 — новий етап глобалізації. URL: https://matrix-info.com/suspilstvo-5-0-novyj-etap- globalizatsiyi/.

29. Величко К.Ю., Цибульська Є.І., Овчаренко К.В. Трансформація бізнес-моделей суб'єктів економічних відносин в цифровій економіці. *Вчені записки ХГУ «НУА».* Том XXIX, 2022. С. 157–170.

30. Тимохова Г.Б., Кудінова М.М. Особливості формування цифрових стратегій розвитку. *Економіко-правові аспекти господарювання: сучасний стан, ефективність та перспективи :* праці VII Міжнар. наук-практ. конф. (Одеса, 25–26 вересня). Одеса, 2022. С. 290–292.

31. Краус К., Краус Н., Осецький В. Суспільство 5.0 на базі розвитку інноваційного університету та цифрового підприємництва. *Економіка та суспільство.* 2021. Вип. 28. DOI: https://doi.org/10.32782/2524-0072/2021-28-37.

32. Fukuyama M. *Society 5.0: Aiming for a New Human-centered Society.* URL: https://www.hitachi.com/rev/ archive/2017/r2017_06/trends/index.html.

33. Марченко О.В., Краус Н.М., Краус К.М. Інноваційне підприємництво і цифровий бізнес: науково- економічна фіча розвитку та зміни в управлінні. *Ефективна економіка*. 2020. № 4. DOI: https://doi.org/ 10.32702/2307-2105-2020.4.

34. Society 5.0. Hitachi and The University of Tokyo Joint Research Laboratory. Springer, Singapore. 2018. DOI:https://doi.org/10.1007/978-981-15-2989-4_9.

35. Криниця С.О. Державна політика цифровізації економіки України. Фінансовий простір. 2018. N3(31) С. 50-57.

36. Скорик О.О., Рябоконь Н.П. Цифрова транс- формація моделі публічного управління: за- рубіжний досвід та вітчизняні реалії. Елек- тронне «Державне управління: удосконален- ня та розвиток». 2020.N7.c.3-17. URL:http:// www.dy.nayka.com.ua/pdf/7_2020/52.pdf).

37. Стратегія сталого розвитку «Україна -2020»: Указ Президента України

від 12 січня 2015 року № 5/2015. URL:https://zakon.rada.gov. ua/laws/show/5/2015#Tex.

38. Про схвалення Концепції розвитку електрон- ного урядування в Україні: розпорядження КМУ від 20 вересня 2017 р. No 649-р. URL: https://zakon.rada.gov.ua/laws/show/649- 2017-р.

39. Про затвердження плану заходів з реалізації Концепції розвитку електронного урядування в Україні: розпорядження КМУ від 22 серпня 2018 р. No 617-р. URL: https://zakon.rada.gov. ua/laws/main/617-2018-р.).

40. Про схвалення Концепції розвитку електрон- ної демократії в Україні та плану заходів щодо її реалізації: розпорядження КМУ від 8 листо- пада 2017 р. No 797-р. URL: https://zakon. rada.gov.ua/laws/main/797-2017-р.).

41. Стеблина Н.О. Складові Цифровізації політики: цифровий форум, цифровий капітал та струк- тура цифрових можливостей/ Науковий жур- нал «Політикус».2020. Випуск 5. с. 126-131.

42. Стратегія сталого розвитку України до 2030 року. URL: https://www.undp.org/uk/ ukraine/publications/стратегія-сталого-розвитку-україни-до-2030-року.

43. Стеблина Н.О. Цифровізації державної політи- ки як дискурс сучасності:Автореф. дисерта- ції на здобуття наукового ступеня доктора політичних наук. Вінниця. 2021. 36 с.

44. Coleman, S., Freelon, D. Introduction: Concep- tualizing Digital Politics. In Handbook of Digi- tal Politics / S. Coleman, D. Freelon – editors. Cheltenham : Edward Elgar, 2015. P. 1–16.

45. Kreiss, D. Digital Opportunity Structures: Ex- plaining Variation in Digital Mobilization during the 2016 Democratic Primaries. In Carpini, Digital Media and Democratic Futures / M. Delli – editor. Philadelphia: University of Pennsylvania. 2019. P. 42–68.

46. Koc-Michalska, K., Lilleker, D. Digital Politics: Mobilization, Engagement, and Participation. Political Communication. 2017. Vol. 34. No 1. P. 1–5. DOI:10.1080/10584609.2016.1243178.

47. Hoff, J., Scheele, C. Theoretical Approaches to Digital Services and Digital Democracy: The Merits of the Contextual New Medium Theory Model. Policy & Internet. 2014. Vol. 6. No 3. P. 241–267. DOI:10.1002/1944-2866. POI368.

48. Gibson, R., Greffet, F., Cantijoch, M. Friend or Foe? Digital Technologies and the Chang- ing Nature of Party Membership. Political Communication. 2017. Vol. 31. No 4. P. 89–111. DOI: 10.1080/10584609.2016.1221011.

49. Національна стратегія сприяння розвит- ку громадянського суспільства в Україні на 2021 – 2026 роки/ Затверджена Указом Пре- зидента Україн від 27 вересня 2021 року № 487/2021/https://www.president.gov.ua/ documents/4872021-40193).

50. Стратегію реформування державного управ- ління України на 2022-2025 роки, розпоряд- женням Кабінету Міністрів України від 21 лип- ня 2021 р. № 831-р. URL:https://zakon.rada. gov.ua/laws/show/831-2021-%D1%80#Text).

51. Cory N. (2020). Surveying the Damage: Why We Must Accurately Measure Cross-Border Data Flows and Digital Trade Barriers. Information Technology and Innovation Foundation, Washington, DC, 27 January. https://itif.org/ publications/2020/01/27/surveying-damage-why-we- must-accuratelymeasure-cross-border-data-flows-and

52. Coyle D. & Nguyen D. (2019). Cloud Computing, Cross-Border Data Flows and New Challenges for Measurement in Economics. *National Institute Eco- nomic Review,* 249(1), 30-38. https://doi.org/10.1177/002795011924900112.

53. Fortune Bunisess Insights (2023). Internet of Thing Market. https://www.fortunebusinessinsights.com/industry- reports/internet-of-things-iot-market-100307

54. IOT Analytics (2023). State of IoT: Number of Connected IoT Devices Growing 16% to 16.7 Billion Globally. https://iot-analytics.com/number-connected- iot-devices

55. ITU Statistics (2023). https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

56. Marcopolo (2023). The Global AI Talent Tracker. https://macropolo.org/digital-projects/the-global-ai- talent-tracker

57. Mazaraki A., Roskladka A., Ivanova O. (2021). China's digital policy: system analysis and implementation prospects for Ukraine. *Вісник КНТЕУ,* 3, 4-17. https://doi.org/10.31617/visnik.knute.2021(137)01

58. Mitchell J., Ker D. & Lesher M. (2021). Measuring the Economic Value of Data. *Going Digital Toolkit Note.* No. 20. https://goingdigital.oecd.org/data/notes/ No20_ToolkitNote_MeasuringtheValueof Data.pdf

59. NTIA (2016). Measuring the Value of Cross-Border Data Flows. United States Department of Commerce, Washington, DC, National Telecommunications and Information Administration. 30 September 2016. https://www.ntia.gov/report/2016/measuring-value- cross-border-data-flows.

60. Speedtest (2023). Median Country Speeds. July. https://www.speedtest.net/global-index

61. Tortois (2023). The Global AI Index. 28 June. https://www.tortoisemedia.com/intelligence/global- ai/#rankings

62. Tsunashima, T. (2020). China Rises as World's Data Superpower as Internet Fractures. November 24. https://asia.nikkei.com/Spotlight/Century-of-Data/China- rises-as-world-s-data-superpower-as-internet-fracturesUNCTAD (2021). Digital Economy Report. *Cross- Border Data Flows And Development: For Whom the Data Flow*. https://unctad.org/system/files/official- document/der2021_en.pdf

63. UNCTAD (2021). Digital Economy Report. *Cross- Border Data Flows And Development: For Whom the Data Flow*. https://unctad.org/system/files/official-document/der2021_en.pdf

64. Voss G. W. (2020). Cross-Border Data Flows, the GDPR, and Data Governance. Washington *International Law Journal.* 29(*3*). 485-532. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3629348

65. Рзаєва С., Рзаєв Д., Роскладка А., Гамалій В. (2023). Моделювання сховища даних штучної нейронної мережі управління бізнесом. *Електронне*

фахове наукове видання "Кібербезпека: освіта, наука, техніка", 4(*20*), 111-123. https://doi.org/10.28925/2663-4023.2023.20.111123

66. Безрук Д.І. Діджиталізація економіки в Україні: проблеми та перспективи. *Вісник Львівського торговельно-економічного університету. Еконо- мічні науки*. 2023. № 71. С. 43−50.

67. Дернова І.А., Боровик Т.М. Цифровізація економіки України в умовах пандемії: тенденції та напрями розвитку. *Economics: time realities*. 2022. № 1 (59). С. 22–29.

68. Ease of doing digital business 2019. URL: https://sites.tufts.edu/digitalplanet/files/2020/03/Ea-se-of-Doing-Digital-Business-2019_2020.pdf

69. European Commission. Shaping Europe's digital future. URL: https://digital-strategy.ec.europa.eu/en/ policies/desi

70. Галущак О., Галущак М., Машлій Г. Цифровізація в Україні: еволюційні перетворення. *Галицький економічний вісник*. 2023. № 2 (81). С. 155−163.

71. IMD World Digital Competitiveness Ranking 2020. URL: https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/

72. IMD World Digital Competitiveness Ranking 2021. URL: https://www.imd.org/uupload/dm/comms/IMD_ World_Digital_Competitiveness_Ranking_2018.pdf

73. IMD World Digital Competitiveness Ranking 2022. URL: https://www.imd.org/research-knowledge/competitiveness/reports/imd-world-digital-competitiveness-ranking-2019/

74. IMD World Digital Competitiveness Ranking 2023. URL: https://imd.cld.bz/IMD-World-Digital- Competitiveness-Ranking-2020/22/

75. IMD World Digital Competitiveness Ranking 2024. URL: https://imd.cld.bz/Digital-Ranking- Report-2021/200/

76. ITU. Committed to connecting the world. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/IDI/de-fault.aspx

77. Подольчак Н.Ю., Білик О.І., Левицька Я.В. Сучасний стан цифровізації в Україні. *Ефективна економіка*. 2019. № 10. URL: http://www.economy.nayka.com.ua/?op=1&z=7300 DOI: 10.32702/2307-2105-2019.10.4).

78. I. Arbidane, H. Purii, A. Mamanazarov, S. Hushko, V. Kulishov, "Digital Transformation Modelling in the Context of Slowbalization", in *Intern. Sc. Congr. Society of Ambient Intelligence (ISC-SAI), Series: Information Technologies and Business Innovations, 100,* 7, *2021*. doi: 10.1051/shsconf/202110001003.

79. Розпорядження Кабінету міністрів України "*Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації*", Київ, 17 січня 2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-p#Text/.

80. Закон України "*Про стимулювання розвитку цифрової економіки в Україні*", Київ, № 2811-IX від 01.12.2022. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text.

81. Національна економічна стратегія України 2030: *Аудит економіки України 2030*. Кабінет міністрів України. URL: https://nes2030.org.ua/#rec246061582.

82. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions 2030. *Digital Compass: The European way for the Digital*, 2021. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52021DC0118

83. Закон України "*Про основні засади забезпечення кібербезпеки України*". *Відомості Верховної Ради (ВВР), 2017, № 45, ст.403.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

84. Указ Президента України "*Про Стратегію кібербезпеки України*". *№ 447/2021. м. Київ, 26 серпня 2021 року.* URL:: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

85. The National Cyber Security Index Ranking (NCSI). "*E-Governance Academy Foundation Company*". URL: https://ncsi.ega.ee/ncsi-index/?type=c.

86. I. Mietule, H. Purii, I. Maksymova, A. Shaikan, S. Hushko, & V. Kulishov, "Digital Humanization of Education in the Light of Geopolitical Challenges" , in: *Society. Integration. Education. Proceedings of the International Scientific Conference*, *1*, 373-384, 2023. doi: 10.17770/sie2023vol1.7160

87. J. M. M. Botelho, I. Mietule, H. Puriy, I. Maksymova, V. Kulishov, "Economic Diplomacy Strategy for the recovery of the slowdown of Globalization (Slowbalization)", in: *Journal of European Economy,* S.l, 20, 2, 246-261, 2021. doi:10.35774/jee2021.02.246.

88. O. Reznikova, "Strategic Analysis of Ukraine's Security Environment", in: *Strategic Panorama*, 2022, 45-53. doi:10.53679/2616-9460.specialissue.2022.05

89. Statista: The global data and business intelligence platform. "*Distribution of detected cyberattacks worldwide in 2022*». URL: https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/.

90. E. Tanriverdiyev, "The State of the Cyber Environment and National Cybersecurity Strategy in Developed Countries", in: *National Security Studies*, 2022, 23, 19-26. doi: 10.37055/sbn/149510.

91. S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, Kim-Kwang R. Choo, "The role of national cybersecurity strategies on the improvement of cybersecurity education", in *Computers & Security*, Volume 119, 102754, 2022. doi: 10.1016/j.cose.2022.102754.

92. International Telecommunication Union (ITU). "*Global Cybersecurity Index 2020*". URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

93. B. J. Blažič, "*Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills*?", in *Educ. Inf. Technol.,* 2021. doi: 10.1007/s10639-021-10704-y.

94. O. Puchkov, O. Uvarkina, "Sustainable development of the system of formal cyber education: reflection of modern concepts", in *Collection* "*Information*

Technology and Security“, *11*(1), 60–68, 2023. doi:10.20535/2411-1031.2023.11.1.283635

95. European Union Agency for Cybersecurity (ENISA). “*Cybersecurity Education Initiatives in the EU Member States*“, 2022. URL: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states.

96. W. Triplett, “Addressing Cybersecurity Challenges in Education“, in *International Journal of STEM Education*, 3, 47-67, 2023. doi:10.52889/ijses.v3i1.132.

97. A. Saed, Al-K. Mousa, & B. Ezedin, “Efforts and Suggestions for Improving Cybersecurity Education“, 1161-1168, 2022. doi:10.1109/EDUCON52537.2022.9766653.

98. R. Nuhan, I. Sairi, N. Zizi, F. Khalid, “The Importance of Cybersecurity Education”, in *School. International Journal of Information and Education Technology*, 10, 378-382, 2022. doi: 10.18178/ijiet.2020.10.5.1393.

99. World Economic Forum. “Which countries spend the most time on social media?”, 2022. URL: https://www.weforum.org/agenda/2022/04/social-media-internet-connectivity/.

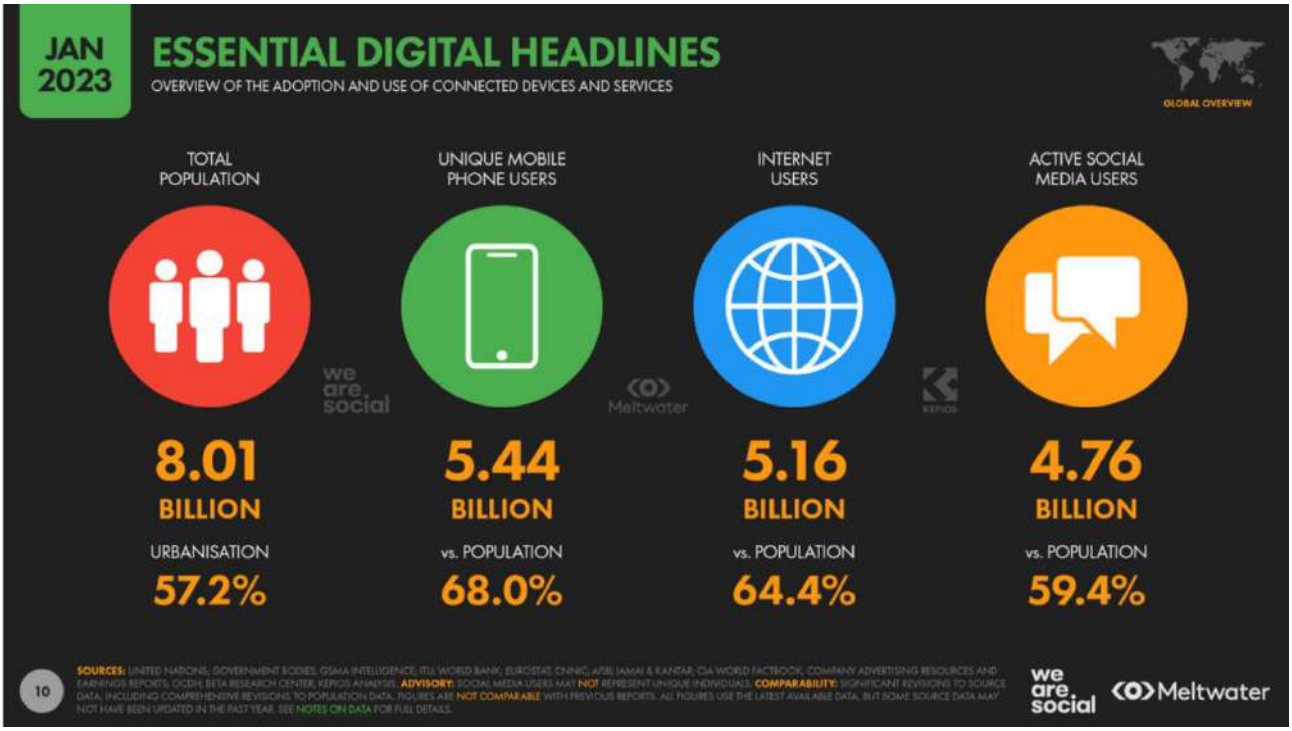
100. The Global AI Index URL: https://www.tortoisemedia.com/intelligence/global-ai#rankings

101. Verbivska, L., Abramova, M., Gudz, M., Lyfar, V., & Khilukha, O. (2023). Digitalization of the Ukrainian economy during a state of war is a necessity of the time. *Amazonia Investiga*, *12*(68), 184-194. https://doi.org/10.34069/AI/2023.68.08.17

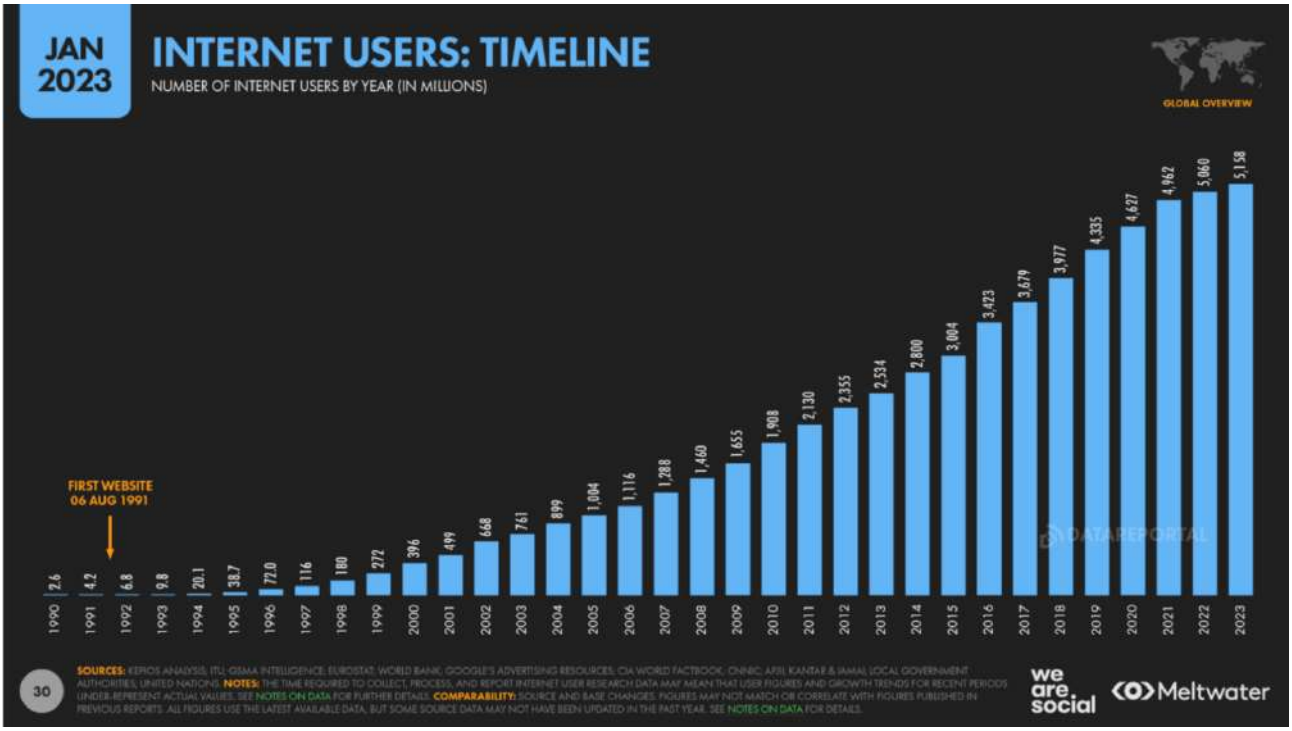
ДОДАТКИ

Додаток А

Кількість інтернет користувачів у світі, 2023 р.



Джерело: (Global Digital 2023).



Джерело: (Global Digital 2023).

Додаток Б

ІНДИКАТОРИ ВИКОНАННЯ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

1. Розробити систему індикаторів стану кібербезпеки, що включатиме: базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Служба безпеки України, Національна академія наук України, Національний інститут стратегічних досліджень
Друге півріччя 2022 року

Індикатор виконання ***Розроблено та представлено НКЦК систему індикаторів стану кібербезпеки.***

Ціль С.1. Дієва кібероборона

2. Створити у системі Міністерства оборони України кібервійська, забезпечивши їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору.

Кабінет Міністрів України, Міністерство оборони України
Перше півріччя 2023 року

Індикатор виконання ***Внесено зміни до законів України «Про Збройні Сили України», «Про оборону України», «Про національну безпеку України», «Про чисельність Збройних Сил України» та до Кримінального кодексу України щодо визначення завдань Кібервійськ Збройних Сил України, збільшення чисельності Збройних Сил України, надання права застосовувати кіберзброю в мирний час та в особливий період, уточнення (доповнення) термінології, встановлення засад військово-цивільного партнерства із фахівцями та суб'єктами господарювання під час організації та проведення кібероперацій.***
Кібервійська Збройних Сил України забезпечено ресурсами за відповідними показниками: персонал, озброєння та військова техніка, запаси, навченість.
Кібервійська як окремий рід військ Збройних Сил України набули спроможностей до виконання завдань за призначенням.

3. Запровадити ефективні механізми взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони.

Міністерство оборони України, Генеральний штаб Збройних Сил України, інші основні суб'єкти національної системи кібербезпеки
Друге півріччя 2023 року

Індикатор виконання ***Міністерством оборони України внесено на розгляд Кабінету Міністрів України проект акта Уряду про затвердження механізму (порядку) взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони (політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі).***

4. Розробити та забезпечити виконання плану кібероборони як складової частини плану оборони України.

Генеральний штаб Збройних Сил України, Міністерство оборони України, інші основні суб'єкти національної системи кібербезпеки
Розробка – друге півріччя 2022 року
Реалізація – постійно

Індикатор виконання ***План кібероборони України як складова частина Плану оборони України розроблено та затверджено.***
Забезпечено скоординоване виконання заходів Плану кібероборони України.
Забезпечено щорічне (за необхідності) уточнення Плану кібероборони України з метою оновлення політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі.

5. Забезпечити проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав – членів НАТО задля досягнення оперативної сумісності.

Міністерство оборони України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші основні суб'єкти національної системи кібербезпеки
Постійно

Індикатор виконання **Проведено щонайменше двічі на рік тематичні навчання, учасниками кожного з яких були представники держав-членів НАТО.**

6. Створити MIL.CERT-UA в інтересах Міністерства оборони України та Збройних Сил України, налагодивши на постійній основі співпрацю із європейською військовою CERT-мережею.

Міністерство оборони України, Генеральний штаб Збройних Сил України
Перше півріччя 2024 року

Індикатор виконання **У Міністерстві оборони України створено MIL.CERT-UA.**
Укладено угоди (меморандуми) щодо співпраці з європейською військовою CERT-мережею.

7. Забезпечити оцінку спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів, оглядів національної системи кібербезпеки та оглядів стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Міністерство оборони України, Генеральний штаб Збройних Сил України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші основні суб'єкти національної системи кібербезпеки
Щороку, починаючи з 2023 року
(за попередній рік), та під час проведення відповідних оглядів

Індикатор виконання ***Кожний із проведених оглядів (оборонних оглядів; оглядів національної системи кібербезпеки; оглядів стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом) містить окремий розділ, в якому надано оцінку спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони.***

8. Запровадити у системі військово-патріотичного виховання та системі територіальної оборони навчальні програми підготовки та проводити практичні навчання у сфері кібербезпеки.

Кабінет Міністрів України, Міністерство оборони України, Генеральний штаб Збройних Сил України, місцеві органи виконавчої влади спільно з органами місцевого самоврядування
Запровадження – перше півріччя
2022 року
Реалізація – постійно

Індикатор виконання ***До кінця першого півріччя 2022 року в навчальних програмах систем військово-патріотичного виховання та територіальної оборони закріплено вимоги до знань слухачів в частині питань кібербезпеки. В подальшому щорічно не менше 25 відсотків учасників цих систем мають бути охоплені такими курсами і здобути практичні навички у сфері кібербезпеки.***

Ціль С.2. Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму

9. Створити відповідно до схвалених концептуальних засад загальнодержавну систему виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури.

Служба безпеки України, Кабінет Міністрів України
Друге півріччя 2024 року

Індикатор виконання ***Розроблено, погоджено із зацікавленими сторонами та впроваджено загальнодержавну систему виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури.***

10. Удосконалити аналітичне і криміналістичне забезпечення контррозвідувального захисту кібербезпеки держави за рахунок впровадження інноваційних методик обробки та оцінки цифрових даних, формування електронних доказів.

Служба безпеки України
Перше півріччя 2023 року

Індикатор виконання ***Розроблено, погоджено із зацікавленими сторонами та затверджено методики обробки та оцінки цифрових даних, формування електронних доказів.***

11. Посилити спроможності у проведенні негласних перевірок стану готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, поступово охопивши такими заходами всі такі об'єкти.

Служба безпеки України
Друге півріччя 2025 року

Індикатор виконання ***Удосконалено нормативно-правову базу щодо проведення негласних перевірок, забезпечено необхідний технічний, апаратно-програмний інструментарій, кадрові спроможності для їх проведення, до кінця 2025 року реалізовано такі перевірки щодо інформаційно-комунікаційних систем всіх об'єктів критичної інфраструктури, ключових державних електронних інформаційних ресурсів, єдиних державних реєстрів та баз даних.***

12. Посилити контррозвідувальний захист сфери електронних комунікацій, ІТ-сфери, афілійованого з ними середовища, спрямований на виявлення, попередження і припинення розвідувально-підривних посягань спецслужб іноземних держав на національну безпеку України у сфері кібербезпеки.

Служба безпеки України
Постійно

Індикатор виконання ***Забезпечено попередження та своєчасне реагування на потенційні загрози національній безпеці, пов'язані із розвідувально-підривною діяльністю спецслужб іноземних держав, спрямованих на сферу електронних комунікацій та ІТ-сферу.***

13. Створити технологічні можливості для автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих об'єктах критичної інфраструктури, їх блокування та визначення пріоритетності.

Служба безпеки України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Міністерство внутрішніх справ України, Міністерство цифрової трансформації України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України
Друге півріччя 2023 року

Індикатор виконання ***Розроблено та затверджено необхідну нормативно-правову базу, інтегровано апаратно-програмні засоби для автоматичного виявлення кібератак у режимі реального часу та їх блокування в***

загальнодержавні інформаційно-комунікаційні системи та на окремі об'єкти критичної інфраструктури, забезпечено автоматизований інформаційний обмін щодо отриманих даних між відповідальними державними органами, формалізовано механізм блокування кібератак.

14. Вдосконалити нормативно-правове, організаційне та кадрове забезпечення загальнодержавної системи боротьби з тероризмом у частині, що стосується залучення правоохоронних органів до здійснення заходів з попередження, виявлення і припинення актів кібертероризму.

Служба безпеки України, Кабінет Міністрів України
Перше півріччя 2024 року

Індикатор виконання ***Протидія та реагування на кібератаки, що створювали небезпеку для життя чи здоров'я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, міжнародними організаціями, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з тією самою метою здійснюється в рамках правового режиму боротьби з тероризмом.***

Ціль С.3. Ефективна протидія кіберзлочинності

15. Завершити імплементацію в законодавство України положень Конвенції про кіберзлочинність.

Кабінет Міністрів України, Служба безпеки України
Друге півріччя 2025 року

Індикатор виконання ***Всі положення Конвенції про кіберзлочинність імплементовано в українське законодавство, створено достатню правову базу для безперешкодної взаємодії із країнами-підписантами Конвенції для ефективної протидії кіберзлочинності в рамках цього міжнародного документу.***

16. Забезпечити унормування в установленому порядку питання щодо електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав – членів ЄС та враховуючи сучасні виклики і тенденції у сфері кібербезпеки.

Кабінет Міністрів України, Служба безпеки України
Друге півріччя 2024 року

Індикатор виконання ***Вітчизняне законодавство забезпечує можливість ефективно використовувати електронні докази у цивільному, адміністративному та кримінальному судочинстві у відповідності до кращих практик Сполучених Штатів Америки, держав – членів ЄС.***

17. Розробити концептуальні підходи щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі (особливо найбільш вразливих груп населення, насамперед дітей).

Міністерство цифрової трансформації України, Міністерство внутрішніх справ України, Національна поліція України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації
Друге півріччя 2022 року

Індикатор виконання ***Чинна державна політика спрямована та сприяє забезпеченню конституційних прав та свобод людини і громадянина під час використання кіберпростору. Розроблено та впроваджено ефективні механізми захисту персональних даних громадян, забезпечення права на повагу до гідності людини і громадянина, свободи слова, недопущення булінгу та використання кіберпростору для сексуальної експлуатації дітей, доведення до самогубства, а також здійснення інших злочинів проти волі, честі та гідності особи, інших прав і свобод людини і громадянина.***

18. Запровадити практику проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів.

Міністерство внутрішніх справ України, Національна поліція України, Міністерство цифрової трансформації України, Міністерство соціальної політики України, Міністерство освіти і науки України, Міністерство культури та інформаційної політики України, Служба безпеки України, Національний банк України
Запровадження – друге півріччя 2022 року
Реалізація – постійно

Індикатор виконання ***Створено нормативні і організаційно-технічні умови для проведення загальнонаціональних інформаційних роз'яснювальних кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами.***
Інформація щодо алгоритму таких дій є загальнодоступною та розміщена на сторінках офіційних Інтернет представництв основних суб'єктів національної системи кібербезпеки.
Забезпечено функціонування цілодобової гарячої лінії, на яку кожен громадянин може звернутися і отримати роз'яснення щодо дій у випадку, якщо він став жертвою кіберзлочину.

19. Розробити методику збору кіберстатистики та щороку оприлюднювати статистичну інформацію щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних сайтах.

Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші основні суб'єкти національної системи кібербезпеки

Розробка – друге півріччя 2023 року

Реалізація – щороку

Індикатор виконання ***Адміністрацією Держспецзв'язку розроблено та затверджено Методику збору кіберстатистики. Основними суб'єктами національної системи кібербезпеки збирається кіберстатистика у відповідності до розробленої Адміністрацією Держспецзв'язку методики. Раз на рік на їх офіційних сайтах публікується інформація щодо кіберінцидентів, кібератак та заходів протидії.***

20. Розробити методику проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, з оцінками ефективності діяльності державних органів у протидії ним і забезпечити проведення таких досліджень.

Кабінет Міністрів України, Національний інститут стратегічних досліджень

Розробка – друге півріччя 2024 року

Реалізація – щороку

Індикатор виконання ***Методика проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, розроблена Держспецзв'язку та затверджена Урядом. Кабінетом Міністрів України організовано щорічне проведення таких досліджень, починаючи з 2024 року.***

21. Розробити методику комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, створити необхідні умови для її практичної реалізації.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Служба безпеки України, Національний інститут стратегічних досліджень

Друге півріччя 2022 року

Індикатор виконання ***Розроблено та затверджено протокольним рішенням НКЦК методику комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам. Зазначена методика використовується на практиці для комунікування між державою і суспільством.***

22. Запровадити механізми ідентифікації суб'єктів електронної комерції у кіберпросторі, забезпечивши внесення відповідних змін до законодавства України.

Кабінет Міністрів України, Національний банк України

Друге півріччя 2025 року

Індикатор виконання ***Чинні організаційно-правові механізми забезпечують ідентифікацію суб'єктів електронної комерції у кіберпросторі.***

23. Забезпечити в установленому порядку врегулювання правового статусу криптовалют.

Кабінет Міністрів України, Національний банк України

Друге півріччя 2023 року

Індикатор виконання ***Розроблено та внесено на розгляд Верховної Ради України законопроект щодо врегулювання правового статусу криптовалют у вітчизняному законодавстві, а також підготовлено відповідні зміни до інших законів та підзаконних нормативно-правових актів.***

24. Проводити спільні з ЄС та НАТО заходи, спрямовані на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози.

Міністерство закордонних справ України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки

Постійно

Індикатор виконання ***Представники України беруть участь не менш ніж у 90% міжнародних заходів ЄС та НАТО у сфері кібербезпеки, на які запрошено українську сторону.***

Україна виступає ініціатором та організатором не менш ніж 7 міжнародних заходів у сфері кібербезпеки щорічно, що проводяться спільно з ЄС та НАТО.

25. Забезпечити підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем та засобів.

Міністерство юстиції України, Міністерство внутрішніх справ України, Служба безпеки України

Друге півріччя 2022 року

Індикатор виконання ***Організовано не менш ніж 5 програм підвищення кваліфікації (тренінгів, семінарів тощо) щорічно із охопленням не менш ніж 80% судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем та засобів.***

Проведено оцінку потреб щодо необхідного апаратно-програмного та іншого забезпечення в інтересах проведення судових експертиз за вказаними напрямами та здійснено його подальшу закупівлю або організоване отримання в рамках міжнародної допомоги.

26. Забезпечити підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів.

Міністерство внутрішніх справ України, Національна поліція України, Служба безпеки України, Державна судова адміністрація України, Офіс Генерального прокурора

Постійно

Індикатор виконання ***Організовано не менш ніж 7 програм підвищення кваліфікації (тренінгів, семінарів тощо) щорічно із охопленням не менш ніж 60% співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів, які працюють у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів.***

27. Залучати приватних експертів до проведення комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів.

Міністерство юстиції України, Міністерство внутрішніх справ України, Національна поліція України, Служба безпеки України, Державна судова адміністрація України, Офіс Генерального прокурора

Постійно

Індикатор виконання ***Нормативно-правова база забезпечує можливість повноцінного залучення приватних експертів.***

У щонайменше 50% випадках проведення розслідувань комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів та у випадках відсутності необхідної кваліфікації та/або технічних можливостей у відповідних державних, у т.ч. правоохоронних органів, було залучено приватних експертів.

Ціль С.4. Розвиток асиметричних інструментів стримування

28. Удосконалити систему розвідувального забезпечення кібербезпеки держави в частині створення, розвитку сил, засобів та інструментів упередження загроз національній безпеці у кіберпросторі.

Служба зовнішньої розвідки України, інші розвідувальні органи України

Друге півріччя 2023 року

Індикатор виконання ***Посилено кадрові та технічні спроможності структурних підрозділів розвідувальних органів, що відповідають за напрям кіберрозвідки та протидії кіберзагрозам національній безпеці.***

29. Посилити заходи щодо забезпечення кібербезпеки інформаційної інфраструктури та кіберзахисту інформаційних ресурсів закордонних дипломатичних установ України та об'єктів державної власності України за кордоном.

Міністерство закордонних справ України, Служба зовнішньої розвідки України, Служба безпеки України, Міністерство оборони України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Перше півріччя 2024 року

Індикатор виконання ***Впроваджено централізовану систему управління кіберінцидентами в структурі МЗС, орієнтовану на забезпечення кіберзахисту інфраструктури та інформаційних ресурсів закордонних дипломатичних установ України та об'єктів державної власності України за кордоном, створено протоколи її спільного використання (МЗС, СБУ, СЗРУ та Держспецзв'язку за загальною координацією НКЦК).***

30. Створити технологічні можливості підключення постачальниками електронних комунікаційних мереж та/або послуг технічних засобів для здійснення оперативно-розшукових, контррозвідувальних та розвідувальних заходів.

Служба безпеки України, розвідувальні органи України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації

Перше півріччя 2024 року

Індикатор виконання ***Налагоджено взаємодію з постачальниками електронних комунікаційних мереж та послуг, забезпечено інтероперабільність наявного у розвідувальних та контррозвідувальних органів технічного обладнання з обладнанням та відповідними протоколами обміну інформацією систем зазначених суб'єктів для підключення технічних засобів для здійснення оперативно-розшукових, контррозвідувальних та розвідувальних заходів.***

31. Запровадити гармонізований з євроатлантичною спільнотою підхід до застосування санкцій у відповідь на підривну діяльність у кіберпросторі, розроблення та узгодження з іноземними партнерами механізму спільних дипломатичних та економічних дій і заходів, зокрема запровадження обмежувальних заходів у вигляді економічних санкцій, у відповідь на деструктивну кібератівність.

Міністерство закордонних справ України, Міністерство економіки України, Служба безпеки України, розвідувальні органи України

Друге півріччя 2022 року

Індикатор виконання ***Країнами ЄС та США в рамках підтримки України та гармонізованого підходу до санаційної політики запроваджено санкції у відповідь на деструктивну кібератівність проти України щодо суб'єктів, до яких запроваджено санкції Україною.***

Аналогічні санкції введено Україною щодо суб'єктів, на які накладено санкції Країнами ЄС та США за деструктивну кіберактивність проти цих країн.

32. Застосовувати усі доступні інструменти дипломатії та міжнародного права задля протидії зловмисній діяльності у кіберпросторі проти України.

Міністерство закордонних справ України
Постійно

Індикатор виконання ***Забезпечено застосування санкцій євроатлантичною спільнотою на рф, юридичних та фізичних осіб рф за зловмисну діяльність у кіберпросторі проти України, застосовано механізм міжнародного судочинства для притягнення рф до відповідальності за кіберзлочини проти України, ініційовано виключення рф з усіх груп та підгруп з кібербезпеки ключових міжнародних організацій (ООН, ОБСЄ, ISO тощо).***

33. Налагодити систематичний обмін інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед Сполученими Штатами Америки, державами – членами ЄС та державами – членами НАТО, створити платформи такого обміну.

Міністерство закордонних справ України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки
Створення платформ – перше півріччя 2023 року
Реалізація – постійно

Індикатор виконання ***Забезпечити автоматизований обмін інформацією в режимі наближеному до реального часу між НКЦК і CERT-UA з боку України та компетентними органами країн ЄС і НАТО щодо кібератак, виявлених вразливостей систем кіберзахисту національного значення, планів та намірів зловмисників щодо реалізації кібероперацій.***

34. Забезпечити розроблення законопроекту, спрямованого на врегулювання питань щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі.

Кабінет Міністрів України, Служба безпеки України
Друге півріччя 2024 року

Індикатор виконання ***Законопроект, спрямований на врегулювання питань щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі, розроблено та внесено на розгляд Верховної Ради України.***

35. Розробити дієві механізми залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі.

Кабінет Міністрів України, Служба безпеки України, розвідувальні органи України
Друге півріччя 2022 року

Індикатор виконання ***Декриміналізовано несанкціоноване втручання в роботу інформаційно-комунікаційних систем з боку фахівців приватного сектору, що здійснюється для стримування та протидії агресії проти України в кіберпросторі у відповідності до вимог закону. Створено кіберрезерв та відпрацьовано механізм його мобілізації. Створено спільноту українських IT-спеціалістів, для нейтралізації ворога в кіберпросторі.***

Ціль К.1. Національна кіберготовність та надійний кіберзахист

36. Розробити Національний план реагування на надзвичайні (кризові) ситуації в кіберпросторі, який визначить механізми реагування на кібератаки загальнонаціонального масштабу щодо об'єктів критичної інформаційної інфраструктури та заходи з подальшого відновлення.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки
Друге півріччя 2023 року

Індикатор виконання ***Розроблено та затверджено Національний план реагування на надзвичайні (кризові) ситуації в кіберпросторі.***

37. Створити національну систему управління інцидентами, розробити та впровадити стандартні операційні процедури для реагування на різні види подій у кіберпросторі з визначенням критеріїв для оцінки критичності подій та пріоритетності реагування залежно від визначеного рівня критичності.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки
Друге півріччя 2023 року

Індикатор виконання ***Створено національну систему управління інцидентами (прийняті відповідні нормативно-правові документи, протестовано функціональність системи).***
Розроблено та впроваджено стандартні операційні процедури для реагування на різні види подій у кіберпросторі.

38. Забезпечити постійний моніторинг національних електронних комунікаційних мереж та інформаційних ресурсів, аналіз вторгнень щодо цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій їх функціонування.

Національний координаційний центр кібербезпеки, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки
Постійно

Індикатор виконання ***Створено нормативні, організаційні та технологічні умови для проведення постійного моніторингу національних електронних комунікаційних мереж та інформаційних ресурсів, аналізу вторгнень щодо цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій їх функціонування.***
Забезпечено на постійній основі обмін інформацією про виявлені в режимі реального часу аномалії функціонування національних електронних комунікаційних мереж та інформаційних ресурсів.

39. Передбачати у проекті закону про Державний бюджет України на відповідний рік видатки на кібербезпеку за окремими бюджетними програмами.

Кабінет Міністрів України, Служба безпеки України, Служба зовнішньої розвідки України
Щороку

Індикатор виконання ***У щорічному Законі України «Про Державний бюджет України» передбачено видатки на кібербезпеку за окремими бюджетними програмами.***

40. Розробити базові (визначатимуть мінімальний обов'язковий рівень) вимоги та рекомендації з питань забезпечення кібербезпеки для державного і приватного секторів з урахуванням кращих світових практик.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші основні суб'єкти національної системи кібербезпеки
Друге півріччя 2024 року

Індикатор виконання ***Розроблені, обговорені із заінтересованими сторонами та затверджені базові вимоги та рекомендації з питань забезпечення кібербезпеки.***

41. Налагодити на основі взаємної довіри системний обмін інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз між усіма суб'єктами забезпечення кібербезпеки, насамперед на базі технологічної платформи Національного координаційного центру кібербезпеки, уніфікувати формати обміну інформацією.

Національний координаційний центр кібербезпеки, Кабінет Міністрів України, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки
Перше півріччя 2023 року

Індикатор виконання ***Уніфіковано формати обміну інформацією (відповідні формати нормативно закріплені).***
Станом на перше півріччя 2023 року щонайменше раз на тиждень відбувається обмін інформацією, учасниками якого є не лише основні суб'єкти національної системи кібербезпеки.

42. Впровадити ризик-орієнтований підхід у частині заходів забезпечення кібербезпеки об'єктів критичної інфраструктури та державних органів, зокрема, розробити методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, забезпечити нормативне врегулювання питань щодо впровадження обов'язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик.

Кабінет Міністрів України, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки
Друге півріччя 2025 року

Індикатор виконання ***Розроблено та затверджено методику ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави.***
Нормативно врегульовано питання щодо впровадження обов'язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик.

43. Впровадити систему сертифікації продукції, яка використовується для функціонування та кіберзахисту інформаційно-комунікаційних систем, насамперед об'єктів критичної інформаційної інфраструктури.

Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України
Друге півріччя 2024 року

Індикатор виконання ***Внесено зміни до переліку***
сфер діяльності, в яких центральні органи виконавчої влади та Служба безпеки України здійснюють функції технічного регулювання.
Створено та акредитовано в Національному агентстві з акредитації України орган з сертифікації продукції, процесів та послуг, орган оцінки відповідності у сфері електронних довірчих послуг та орган з оцінки відповідності у сфері криптографічного захисту інформації. Забезпечено функціонування зазначених органів та випробувальної лабораторії.
Розширено сфери акредитації органу з сертифікації продукції у сфері кіберзахисту.

44. Забезпечити розвиток організаційно-технічної моделі кіберзахисту.

Адміністрація Державної служби спеціального зв'язку та захисту інформації України, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки
Затвердження моделі – друге півріччя 2022 року
Реалізація – постійно

Індикатор виконання ***До завершення 2022 року розроблено перелік нормативно-правових актів, необхідних для розвитку організаційно-технічної моделі кіберзахисту.***

У першому півріччі 2023 року визначено необхідні заходи, етапи їх реалізації та відповідальні суб'єкти, які забезпечують розвиток елементів організаційно-технічної моделі кіберзахисту у різних інфраструктурах та їх рівнях.
У 2024 – 2025 роках забезпечено впровадження складових частин організаційно-технічної моделі кіберзахисту.

45. Завершити процеси визначення об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, створити і забезпечити функціонування державного реєстру об'єктів критичної інформаційної інфраструктури, постійно переглядати та оновлювати вимоги до їх кіберзахисту з урахуванням сучасних міжнародних стандартів з питань кібербезпеки.

Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Національний банк України, інші суб'єкти національної системи захисту критичної інфраструктури

Друге півріччя 2022 року

Індикатор виконання

Затверджено Перелік об'єктів критичної інфраструктури.
Затверджено Перелік об'єктів критичної інформаційної інфраструктури.
Через два місяці після затвердження Преліку ОКІ прийнято, розроблено в рамках міжнародної технічної допомоги спеціалізоване програмне та апаратне забезпечення Реєстру ОКІІ.
Створено макет Реєстру ОКІІ, затверджено технічне завдання на КСЗІ інфрамаційно-комунікаційної системи (ІКС) «Реєстр ОКІІ»
І півріччя 2023 року
Проведено тестову експлуатацію та усунено недоліки макету ІКС «Реєстр ОКІ».
Розроблено експлуатаційну документацію, проведено навчання персоналу адміністраторів Реєстру ОКІІ, створено та підтверджено відповідність КСЗІ ІКС «Реєстру ОКІІ».
ІІ півріччя 2023 року
ІКС «Реєстр ОКІ» уведено в експлуатацію наказом розпорядника Національного реєстру ОКІ.
І півріччя 2024 року
Впроваджено подання поточних профілів кіберзахисту ОКІІ до Реєстру ОКІІ, створено поточний профіль кіберзахисту ІКС «Реєстр ОКІІ».
ІІ півріччя 2022 року
Розроблено зміни до Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 р. № 518, в яких запроваджено вимоги щодо оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів.
Переглянуто та за необхідності оновлено вимоги до кіберзахисту об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів.

46. Запровадити на постійній основі оцінку стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, встановити обов'язковість та періодичність проведення такої оцінки з урахуванням категорій критичності об'єктів, стимулювати участь у цих заходах фахівців з кібербезпеки приватного сектору.

Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Служба безпеки України

Розробка змін до законодавства – друге півріччя 2022 року
Реалізація – постійно

Індикатор виконання

Нормативно визначено* обов'язковість та періодичність проведення оцінки стан*у захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, а також порядок залучення до таких заходів фахівців з кібербезпеки приватного сектору.

47. Впровадити систему аудиту інформаційної безпеки, насамперед на об'єктах критичної інфраструктури, визначити механізми та базові методики проведення аудитів, встановити вимоги до аудиторів інформаційної безпеки, їх сертифікації, атестації (переатестації), навчання та підвищення кваліфікації, а також щодо обов'язковості та періодичності проведення аудитів, надання узагальненої інформації про результати аудитів до Національного координаційного центру кібербезпеки.

Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Служба безпеки України

Друге півріччя 2022 року

Індикатор виконання

Прийнято постанову Кабінету Міністрів України "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури".
Затверджено наказами Адміністрації Держспецзв'язку Методичні рекомендації щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; Вимоги до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та Порядок атестації (переатестації) аудиторів інформаційної безпеки на об'єктах критичної інфраструктури.

48. Забезпечити розвиток систем технічного і криптографічного захисту інформації, пріоритетність використання засобів технічного і криптографічного захисту інформації вітчизняного виробництва для кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Служба безпеки України.
Постійно

Індикатор виконання ***Розроблено та прийнято нормативний документ, що створює передумови пріоритетності використання засобів технічного і криптографічного захисту інформації вітчизняного виробництва.***
Щорічно кількість засобів ТЗІ/КЗІ вітчизняного виробництва з підтвердженою відповідністю збільшується.
Щорічно зростає експорт вітчизняних засобів ТЗІ/КЗІ.

49. Впровадити вітчизняні рішення із захисту інформації.

Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Служба безпеки України
Постійно

Індикатор виконання ***В органах державної влади та на об'єктах критичної інформаційної інфраструктури за умови існування декількох рішень із захисту інформації з однаковим характеристиками пріоритетність віддана вітчизняним.***

50. Проводити командно-штабні кібернавчання стратегічного рівня, а також тематичні кібернавчання та тренінги за участю представників державного та приватного секторів.

Національний координаційний
центр кібербезпеки, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші основні суб'єкти національної системи кібербезпеки
Постійно

Індикатор виконання ***Щонайменше раз на рік проводяться командно-штабні кібернавчання стратегічного рівня.***
Щонайменше раз на 2 роки проводяться тематичні кібернавчання та тренінги за участю представників державного та приватного секторів.

51. Забезпечити розвиток мережі центрів реагування на кібератаки та кіберінциденти.

Кабінет Міністрів України, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки
Друге півріччя 2025 року

Індикатор виконання ***Щорічно вводиться в роботу щонайменше один новий центр (секторальний або відомчий) реагування на кібератаки та кіберінциденти.***

52. Завершити розгортання Національної телекомунікаційної мережі, збільшити її пропускну здатність, передбачити під час її функціонування використання виключно вітчизняних засобів криптографічного захисту інформації.

Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України
Друге півріччя 2022 року

Індикатор виконання ***Завершено розгортання Національної телекомунікаційної мережі.***
Збільшено пропускну здатність транспортної платформи Національної телекомунікаційної мережі шляхом нарощування її оптичного сегмента за рахунок:
збудовано п'ять вузлів Національної телекомунікаційної мережі для чотирьох центральних органів виконавчої влади та Головного управління урядового фельд'єгерського зв'язку Держспецзв'язку;
спроектовано та збудовано ВОЛЗ транспортної платформи Національної телекомунікаційної мережі до адміністративних будівель територіальних органів державної влади, складових сектору безпеки і оборони в обласних центрах України (за окремим планом).

53. Забезпечити функціонування та розвиток Національного центру резервування державних інформаційних ресурсів, провести модернізацію системи захищеного доступу державних органів до мережі Інтернет.

Адміністрація Державної служби спеціального зв'язку та захисту інформації України
Постійно
Модернізація системи захищеного доступу державних органів до мережі Інтернет – друге півріччя 2023 року

Індикатор виконання ***Забезпечено функціонування та розвиток Національного центру резервування державних інформаційних ресурсів.***
Розроблено технічне завдання та проведено модернізацію системи захищеного доступу державних органів до мережі Інтернет.

54. Створити національний сервіс доменних імен (DNS).

Кабінет Міністрів України, Національний координаційний
центр кібербезпеки
Перше півріччя 2023 року

Індикатор виконання ***Створено та введено в експлуатацію національний сервіс доменних імен (DNS).***

Ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки

55. Забезпечити координацію наукового співтовариства під час проведення наукових досліджень і розробок у сфері кібербезпеки та залучення його до заходів з реалізації державної політики у сфері кібербезпеки.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Міністерство освіти і науки України, Національна академія наук України, Національний інститут стратегічних досліджень
Створення механізму координації – друге півріччя 2022 року
Реалізація – постійно

Індикатор виконання ***До кінця другого півріччя 2022 року створено (розроблено загальне бачення та реалізовано на практиці) координаційний механізм. Координаційні заходи відбуваються не рідше 4 разів на рік. Річні результати координаційних заходів подаються до НКЦК.***

56. Визначити довгострокові напрями проведення досліджень і розробок у сфері кібербезпеки, а також розробити дієву програму державної підтримки (на основі проектного підходу) стратегічно важливих для кібербезпеки держави наукових установ і організацій, проведення наукових досліджень у цій сфері для потреб національної безпеки і оборони.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Міністерство освіти і науки України, Національна академія наук України, Національний інститут стратегічних досліджень
Визначення довгострокових напрямів – друге півріччя 2022 року
Розроблення програми – перше півріччя 2023 року

Індикатор виконання ***До кінця другого півріччя 2022 року визначено та передано до НКЦК перелік (з короткою анотацією) довгострокових напрямів проведення досліджень і розробок у сфері кібербезпеки. До кінця першого півріччя 2023 року розроблено Концепцію державної цільової програми підтримки стратегічно важливих для кібербезпеки держави наукових установ і організацій, проведення наукових досліджень у цій сфері для потреб національної безпеки і оборони.***

57. Забезпечити стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням розвитку новітніх інформаційно-комунікаційних технологій, зокрема, технологій хмарних та квантових обчислень, 5G-мереж, Інтернету речей, штучного інтелекту, а також появи нових засобів реалізації кіберзагроз з метою створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, Національна академія наук України
Розроблення механізму стимулювання – друге півріччя 2022 року
Реалізація – постійно

Індикатор виконання ***До кінця другого півріччя 2022 року розроблено (створено концептуальне бачення, затверджено необхідні нормативно-правові документи та проведено пілотне застосування) механізму стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням розвитку новітніх інформаційно-комунікаційних технологій. Щорічно механізм забезпечує стимулювання мінімум одного нового дослідження чи розробки в наступних категоріях: технології хмарних та квантових обчислень, 5G-мережі, Інтернет речей, штучний інтелект, нові засоби реалізації кіберзагроз, створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки. Щорічно до НКЦК подається довідкова інформація про результативність застосування механізму.***

58. Удосконалити систему підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки.

Кабінет Міністрів України, Міністерство освіти і науки України, Національне агентство України з питань державної служби, основні суб'єкти національної системи кібербезпеки
Розроблення концепції системи – друге півріччя 2022 року
Реалізація концепції – друге півріччя 2025 року

Індикатор виконання ***До кінця другого півріччя 2022 року розроблено та публічно презентовано Концепцію системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки. До кінця другого півріччя 2025 року Концепція офіційно прийнята, має затверджений план реалізації та впроваджується щонайменше в пілотному режимі.***

59. Розробити Загальнонаціональну програму кіберграмотності, спрямовану на підвищення рівня цифрової грамотності населення України, зокрема, шляхом включення питань стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії ним до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти.

Кабінет Міністрів України, Міністерство освіти і науки України, Міністерство цифрової трансформації України, основні суб'єкти національної системи кібербезпеки
Розробка програми – перше півріччя 2023 року
Реалізація програми – постійно

Індикатор виконання ***До кінця першого півріччя 2023 року розроблено деталізовану Загальнонаціональну програму кіберграмотності. Щорічно програма охоплює щонайменше на 10% цільових аудиторій більше, ніж у попередньому році.***

60. Утворити центри, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері.

Кабінет Міністрів України, Національна академія наук України, основні суб'єкти національної системи кібербезпеки
Друге півріччя 2025 року

Індикатор виконання ***Створено щонайменше 3 центри (відомчі, секторальні, наукові або інші), які на постійній основі здійснюють узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері (або хоча б одне з цих завдань).***

61. Забезпечити матеріальне стимулювання фахівців у сфері кібербезпеки, які перебувають на військовій, державній службі, у тому числі на державній службі особливого характеру, службі в правоохоронних органах або працюють за трудовим договором у державному секторі і безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, з урахуванням рівнів оплати праці таких фахівців у приватному секторі.

Кабінет Міністрів України, основні суб'єкти національної системи кібербезпеки
Перше півріччя 2022 року

Індикатор виконання ***Розроблено та прийнято акт(и) Кабінету Міністрів України, що забезпечать матеріальне стимулювання фахівців у сфері кібербезпеки, які перебувають на військовій, державній службі, у тому числі на державній службі особливого характеру, службі в правоохоронних органах або працюють за трудовим договором у державному секторі і безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, з урахуванням рівнів оплати праці таких фахівців у приватному секторі.***

62. Залучити суб'єктів національної системи кібербезпеки до міжнародних програм навчання і підвищення кваліфікації персоналу.

Міністерство закордонних справ України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки
Постійно

Індикатор виконання ***Щорічно ініціюється (направлено запит, проведено консультації) приєднання України до щонайменше однієї нової міжнародної програми навчання і підвищення кваліфікації персоналу.***
Щорічно щонайменше 5 представників основних суб'єктів національної системи кібербезпеки та ОКІ проходять навчання/підвищення кваліфікації за міжнародними програмами.

Ціль К.3. Безпечні цифрові послуги

63. Зміцнювати довіру приватного сектору та громадян до цифрових послуг, які надаються державою, безумовно виконуючи вимоги щодо забезпечення кібербезпеки та кіберзахисту під час їх надання та інформуючи громадськість про їх безпечність та надійність.

Міністерство цифрової трансформації України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, інші центральні та місцеві органи виконавчої влади, Національний банк України
Постійно

Індикатор виконання ***Щорічне проведення роз'яснювальних інформаційних кампаній, що охоплюють до 20% представників цільових аудиторій.***

64. Забезпечити впровадження цифрових послуг для населення та розвиток національної інформаційної інфраструктури.

Кабінет Міністрів України, Міністерство цифрової трансформації України, Національний банк України
Постійно

Індикатор виконання ***Щорічно впроваджується щонайменше 5 нових цифрових послуг.***
95% закладів соціальної інфраструктури та органів місцевого самоврядування підключені до широкосмугового доступу до мережі Інтернет із швидкістю не менше 100 Мбіт/с.

65. Розробити національні стандарти у сфері кібербезпеки, організаційні та технічні вимоги, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів.

Адміністрація Державної служби спеціального зв'язку та захисту інформації України,
Міністерство економіки України, основні суб'єкти національної системи кібербезпеки
Друге півріччя 2025 року

Індикатор виконання ***Розроблено та прийнято національні стандарти, гармонізовані із європейськими/міжнародними стандартами у сфері кібербезпеки в частині безпеки інтернету речей, застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень.***

66. Створити органи з оцінки відповідності надавачів електронних довірчих послуг вимогам для кваліфікованих надавачів кваліфікованих електронних довірчих послуг.

Кабінет Міністрів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Міністерство цифрової трансформації України, Національний банк України
Перше півріччя 2023 року

Індикатор виконання ***Створено (прийнята необхідна нормативно-правова база, забезпечено організаційні, технічні, кадрові та фінансові спроможності) щонайменше два органи з оцінки відповідності надавачів електронних довірчих послуг.***

67. Створити необхідні передумови (нормативні, організаційні, технологічні) для автентифікації користувачів сервісів цифрових послуг (там, де це потрібно) за допомогою інтегрованої системи електронної ідентифікації з використанням технологій електронної ідентифікації та/або електронних довірчих послуг.

Міністерство цифрової трансформації України
Друге півріччя 2022 року

Індикатор виконання ***Створено та впроваджено інтегровану систему електронної ідентифікації з використанням технологій електронної ідентифікації та/або електронних довірчих послуг.***

68. Підвищити ефективність системи захисту персональних даних громадян шляхом гармонізації законодавства України з відповідним законодавством ЄС та посилення відповідальності за порушення встановлених вимог.

Кабінет Міністрів України, Уповноважений Верховної Ради України з прав людини (за згодою)
Друге півріччя 2023 року

Індикатор виконання ***До національного законодавства імплементовано положення GDPR.***

Ціль В.1. Зміцнення системи координації

69. Розробити та затвердити порядок проведення огляду національної системи кібербезпеки, забезпечивши його проведення не менше ніж раз на рік протягом реалізації Стратегії.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки
Затвердження порядку – друге півріччя 2022 року
Проведення огляду – щороку, починаючи з 2023 року

Індикатор виконання ***Протокольним рішенням НКЦК затверджено порядок проведення огляду національної системи кібербезпеки. Кабінетом Міністрів України спільно з НКЦК організовано щорічне проведення такого огляду відповідно до затвердженого порядку.***

70. Запровадити обов'язкове негайне, без невиправданої затримки, надання інформації про кіберзагрози, кібератаки та кіберінциденти всіма відомчими та галузевими (секторальними) центрами кібербезпеки (кіберзахисту) до Національного координаційного центру кібербезпеки.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки
Встановлення вимог та відповідальності щодо інформування – друге півріччя 2022 року
Реалізація – постійно

Індикатор виконання ***Усі відомчі та галузеві (секторальні) центри кібербезпеки (кіберзахисту) повідомили НКЦК про 100% кібератак, які були виявлені ними протягом всього періоду виконання Стратегії відповідно до наступних параметрів:***
відомчі та галузеві (секторальні) центри кібербезпеки (кіберзахисту) невідкладно, не пізніше 30 хвилин з моменту виявлення, інформують Національний координаційний центр кібербезпеки про виявлену кібератаку або кіберінцидент, що потенційно може мати критичні наслідки для кібербезпеки держави із зазначенням об'єкта кібератаки (кіберінциденту), часу її здійснення та іншої наявної інформації. Протягом 12 годин після виявлення такої кібератаки/кіберінцидента у встановленому порядку НКЦК надається технічна інформація (індикатори компрометації, тип атаки, особливості механізму реалізації тощо), а також інформація щодо можливого джерела, потенційних наслідків, додаткових обставин, вжитих та запланованих заходів реагування.

71. Забезпечити розгляд найважливіших питань у сфері кібербезпеки України на засіданнях Національного координаційного центру кібербезпеки, системний контроль за станом виконання його рішень.

Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки
Постійно

Індикатор виконання ***Засідання Національного координаційного центру кібербезпеки, а також його робочих груп проводяться на системній основі, але не рідше одного разу на квартал. На засіданнях розглядаються найважливіші питання у сфері кібербезпеки України та приймаються стратегічні рішення. Контроль за їх виконанням забезпечено Апаратом РНБО України.***

72. Запровадити скоординоване виявлення та розкриття вразливостей інформаційно-комунікаційних систем.

Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки
Впровадження системи управління вразливостями – друге півріччя 2023 року
Реалізація – постійно

Індикатор виконання ***Створено нормативно-правову базу та організаційні механізми щодо скоординованого виявлення та розкриття вразливостей інформаційно-комунікаційних систем, впроваджено систему управління вразливостями. Виявлення та розкриття вразливостей інформаційно-комунікаційних систем здійснюється на системній основі відповідальними суб'єктами забезпечення кібербезпеки із залученням приватного сектору.***

73. Розробити та запровадити механізми заохочення приватного сектору, наукового співтовариства, громадських організацій та окремих громадян до участі у формуванні та реалізації заходів із забезпечення кібербезпеки.

Кабінет Міністрів України, основні суб'єкти національної системи кібербезпеки, Національний інститут стратегічних досліджень
Перше півріччя 2024 року

Індикатор виконання ***Розроблено та впроваджено організаційно-правові механізми заохочення приватного сектору, наукового співтовариства, громадських організацій та окремих громадян до участі у формуванні та реалізації заходів із забезпечення кібербезпеки.***

74. Забезпечити щорічне оприлюднення основними суб'єктами національної системи кібербезпеки публічних звітів про стан кібербезпеки за сферами відповідальності.

Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки
Щороку, починаючи з 2022 року
(за попередній рік)

Індикатор виконання ***Публічні звіти про стан кібербезпеки за сферами відповідальності щорічно оприлюднюються на офіційних веб-сайтах основних суб'єктів національної системи кібербезпеки***.

Ціль В.2. Формування нової моделі відносин у сфері кібербезпеки

75. Забезпечити розроблення законопроекту, спрямованого на врегулювання питань державно-приватного партнерства у сфері кібербезпеки, визначивши форми і методи здійснення такого партнерства, зміцнивши взаємну довіру та передбачивши можливість запровадження експериментальних проектів у цій сфері.

Кабінет Міністрів України, Служба безпеки України
Перше півріччя 2023 року

Індикатор виконання ***Розроблено та внесено на розгляд Верховної Ради України законопроект.***

76. Запровадити проведення на регулярній основі консультацій заінтересованих сторін та надання методичної допомоги з питань утворення підрозділів кіберзахисту, галузевих (секторальних) центрів забезпечення кібербезпеки та команд реагування на кіберінциденти, всебічно сприяти їх розвитку.

Національний координаційний центр кібербезпеки, Адміністрація Державної служби спеціального зв'язку та захисту інформації України
Постійно

Індикатор виконання ***Створено механізм проведення консультацій, який застосовується на постійній основі.***

77. Залучати на регулярній основі представників наукових установ, громадських організацій та незалежних експертів у сфері кібербезпеки до розроблення проектів нормативно-правових актів, нормативних документів та стандартів у цій сфері.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки
Постійно

Індикатор виконання ***Щорічно до розробки проектів НПА, нормативних документів та стандартів у цій сфері залучається мінімум один новий (такий, що не залучався до того протягом реалізації Стратегії) представник наукових установ/ громадських організацій/незалежний експерт.***

78. Підвищити ефективність залучення громадськості до прийняття рішень у сфері кібербезпеки шляхом проведення відповідних опитувань (анкетувань) та розміщення їх результатів на інформаційних ресурсах Національного координаційного центру кібербезпеки та основних суб'єктів національної системи кібербезпеки.

Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки
Постійно

Індикатор виконання ***Щорічно на сайті НКЦК розміщується щонайменше одна нова анкета (опитування) з актуальних питань кібербезпеки.***

79. Стимулювати розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом, що пріоритетно використовуватимуться для обробки та захисту державних інформаційних ресурсів, а також на об'єктах критичної інформаційної інфраструктури.

Кабінет Міністрів України, Міністерство цифрової трансформації України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України
Постійно

Індикатор виконання ***Запроваджено (прийняті необхідні НПА, забезпечено організаційні та фінансові можливості) механізм стимулювання розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом.***
Щорічно надається підтримка щонайменше трьом вітчизняним програмним продуктам, що використовуватимуться для обробки та захисту державних інформаційних ресурсів, а також на об'єктах критичної інформаційної інфраструктури.

80. Впровадити програму розвитку ринку товарів і послуг у сфері кібербезпеки, що включатиме стимулювання його розвитку та міжнародного визнання.

Кабінет Міністрів України
Друге півріччя 2024 року

Індикатор виконання ***Розроблено та впроваджено (прийняті необхідні НПА, забезпечено організаційні та фінансові можливості) програму розвитку ринку товарів і послуг у сфері кібербезпеки.***

81. Продовжити практику щорічного проведення місяця кібербезпеки в Україні із залученням широкого кола профільних фахівців та експертів державних органів, закладів освіти та наукових установ, а також громадських об'єднань та приватного сектору.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки
Щороку у жовтні

Індикатор виконання ***Щорічно проводяться заходи, присвячені місяцю кібербезпеки в Україні.***
Щорічно за результатами проведення місяця кібербезпеки готується інформаційна довідка, яка відображає: коло залучених профільних фахівців та експертів державних органів, закладів освіти та наукових установ, а також громадських об'єднань та приватного сектору.

82. Запровадити систему страхування від кіберризиків, зокрема механізм оцінки втрат суб'єктів господарювання внаслідок кібератак для можливості їх відшкодування.

Кабінет Міністрів України
Друге півріччя 2025 року

Індикатор виконання ***Розроблено та прийнято НПА, що дозволяє реалізувати в Україні систему страхування від кіберризиків, зокрема механізм оцінки втрат суб'єктів господарювання внаслідок кібератак для можливості їх відшкодування.***
Запроваджено щонайменше один пілотний проект.

83. Розробити фінансові та нефінансові механізми для сприяння впровадженню сучасних технологій кібербезпеки у державному і приватному секторі, включаючи страхування, лізинг, пільги тощо.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки
Перше півріччя 2025 року

Індикатор виконання ***Розроблені та запроваджені (прийняті необхідні НПА, забезпечено організаційні та фінансові можливості) фінансові та нефінансові механізми.***
Хоча б один з механізмів функціонує в пілотному режимі.

Ціль В.3. Прагматичне міжнародне співробітництво

84. Забезпечити участь України у міжнародних заходах ООН щодо заохочення відповідальної поведінки держав у кіберпросторі.

Міністерство закордонних справ України
Постійно

Індикатор виконання ***Щорічно забезпечується участь представників України у 100% заходів ООН щодо заохочення відповідальної поведінки держав у кіберпросторі.***
Щорічно надається перелік заходів із зазначеного питання, які відбувались під егідою ООН та хто і в якому статусі приймав в них участь від України.

85. Забезпечити участь України у доопрацюванні Другого додаткового протоколу до Конвенції про кіберзлочинність щодо вироблення заходів та гарантій для вдосконалення міжнародної співпраці між правоохоронними та судовими органами, а також між органами влади та постачальниками послуг в інших державах.

Міністерство закордонних справ України
Постійно

Індикатор виконання ***Представник(и) України постійно приймають участь у заходах із доопрацювання Другого додаткового протоколу до Конвенції про кіберзлочинність.***
Щорічно надається інформація про кількість заходів, а також хто і в якому статусі приймав в них участь від України.

86. Розширити шляхом діалогу з міжнародними партнерами доступ правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю, до телекомунікаційної системи Інтерполу I-24/7.

Національна поліція України, Служба безпеки України, Міністерство закордонних справ України
Перше півріччя 2023 року

Індикатор виконання ***Правоохоронні органи України, з числа основних суб'єктів національної системи кібербезпеки, мають постійний доступ до ресурсів Європейського центру боротьби з кіберзлочинністю та до телекомунікаційної системи Інтерполу I-24/7.***

87. Продовжити співробітництво з Агентством Європейського Союзу з питань мережевої та інформаційної безпеки, зокрема з питань скоординованого розкриття вразливостей та імплементації Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу як елементу євроінтеграції України.

Кабінет Міністрів України, Служба безпеки України
Постійно

Індикатор виконання ***Щорічно проводяться щонайменше одні консультації між представниками України та Агентства Європейського Союзу з питань мережевої та інформаційної безпеки.***

88. Поглибити співпрацю з Міжнародним союзом електрозв'язку у сферах кібербезпеки та електронних комунікацій, зокрема з питань стандартизації у цих сферах.

Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації
Друге півріччя 2022 року

Індикатор виконання ***Забезпечено участь у заходах Міжнародного союзу електрозв'язку у сферах кібербезпеки та електронних комунікацій щодо питань стандартизації і удосконалення національної системи електронних комунікацій.***

89. Розвивати практичне співробітництво з НАТО щодо питань кібероборони, налагодити тісну взаємодію з цих питань із відповідними структурами Альянсу, зокрема Радою управління з кібероборони (NATO Cyber Defence Management Board), Центром операцій у кіберпросторі (Cyberspace Operations Centre), Центром можливостей з реагування на комп'ютерні інциденти (NATO Computer Incident Response Capability), Об'єднаним центром передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence).

Національний координаційний центр кібербезпеки, Міністерство оборони України, Генеральний штаб Збройних Сил України, основні суб'єкти національної системи кібербезпеки
Постійно

Індикатор виконання ***Україна має офіційне представництво у всіх вказаних структурах (або підписані угоди (меморандуми) про співробітництво).***
З кожною організацією визначено коло питань для практичної співпраці.
З кожною організацією є щонайменше один спільний реалізований проект станом на кінець 2025 року.

90. Поглибити співпрацю з міжнародними організаціями у сфері захисту дітей від сексуального онлайн-насильства.

Міністерство цифрової трансформації України, Національна поліція України
Постійно

Індикатор виконання ***Спільно з міжнародними партнерами щорічно проводиться не менше 5 заходів, спрямованих на захист дітей від сексуального онлайн-насильства.***
Щорічно реалізується щонайменше один пілотний проект.

91. Забезпечити розвиток міжнародного співробітництва у сфері кібербезпеки шляхом підтримки міжнародних ініціатив у цій сфері, які відповідають національним інтересам України.

Міністерство закордонних справ України, Національний координаційний центр кібербезпеки
Постійно

Індикатор виконання ***Щорічно Україна підтримує щонайменше одну міжнародну ініціативу.***

92. Продовжити практику проведення двосторонніх кібердіалогів з державами – партнерами з метою обміну передовим досвідом у сфері кібербезпеки, інформацією про кіберзагрози, розвитку комунікації між заінтересованими державними органами України та іноземних держав, розширити коло держав – партнерів, з якими проводяться кібердіалоги, ініціювати питання щодо укладення двосторонніх договорів про співпрацю у сфері кібербезпеки.

Міністерство закордонних справ України
Постійно

Індикатор виконання ***Щорічно проводяться кібердіалоги з наявними партнерами, а також щорічно додається щонайменше одна країна для таких діалогів.***

93. Створити постійно діючу робочу групу з питань взаємодії із провідними IT-компаніями, світовими провайдерами цифрових послуг, соціальними мережами з метою протидії гібридним загрозам, поширенню дезінформації, можливості застосування санкцій відповідно до законів України.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки, основні суб'єкти національної системи кібербезпеки
Перше півріччя 2023 року

Індикатор виконання ***Створено постійно діючу робочу групу, проведено щонайменше одне засідання робочої групи.***

94. Визначити та затвердити перелік пріоритетних напрямів залучення міжнародної технічної допомоги у сфері кібербезпеки України.

Кабінет Міністрів України, Національний координаційний центр кібербезпеки
Друге півріччя 2022 року.

Індикатор виконання ***Підготовлено та затверджено список пріоритетних напрямів, проведено щонайменше одні консультації щодо їх підтримки за рахунок міжнародної технічної допомоги.***