ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут менеджменту та підприємництва

Кафедра публічного управління та адміністрування
Ступінь вищої освіти «Магістр»
Спеціальність 281 «Публічне управління та адміністрування»
Освітньо-професійна програма «Публічне управління та адміністрування»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ірина АНТИПЕНКО
«25» травня 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Павлюка Юрія Андрійовича

1. Тема роботи **«Теоретичні та практичні аспекти державної політики у сфері інформаційного суспільства в Україні»**;
керівник кваліфікаційної роботи – Панченко Олег Анатолійович,
доктор наук з публічного управління, професор, затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467.
2. Термін подання кваліфікаційної роботи – «22» грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: спеціальна теоретична і методична наукова література; наукові публікації (статті, монографії, дисертаційні дослідження) провідних вітчизняних та закордонних дослідників за темою кваліфікаційної роботи; результати науково-дослідної роботи кафедри публічного управління та адміністрування «Теоретико-прикладні аспекти розвитку цифрової держави в Україні»; нормативно-правові документи; матеріали переддипломної практики.
4. Перелік ілюстративного матеріалу: презентація
5. Дата видачі завдання: «27» червня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Структура роботи, вступ	27.06.25 - 29.08.25	Виконано
Розділ 1	01.09.25 - 26.09.25	Виконано
Розділ 2	29.09.25 - 24.10.25	Виконано
Розділ 3	27.10.25 - 28.11.25	Виконано
Висновки, додатки	01.12.25 - 12.12.25	Виконано
Презентація	15.12.25 - 19.12.25	Виконано

Здобувач вищої освіти _____ Юрій ПАВЛЮК

Керівник
кваліфікаційної роботи _____ Олег ПАНЧЕНКО

РЕФЕРАТ

Павлюк Ю. А. Теоретичні та практичні аспекти державної політики у сфері інформаційного суспільства в Україні : кваліф. робота на здобуття освіт. ступеня магістра; спец. 281 «Публічне управління та адміністрування»; Держ. у-т інформац.-комунікац. технолог.; наук. керівник О.А.Панченко, д.н.з публ.упр., професор; Київ, 2025.; 121 с.

Метою кваліфікаційної роботи є комплексне дослідження теоретичних засад формування та аналіз практичних аспектів реалізації державної політики у сфері інформаційного суспільства в Україні, а також розробка науково обґрунтованих пропозицій та рекомендацій щодо її удосконалення з урахуванням сучасних глобальних викликів та європейського досвіду.

Об'єктом дослідження є державна політика України у сфері інформаційного суспільства та цифровізації (включаючи розвиток електронного урядування, забезпечення кібербезпеки та подолання цифрового розриву).

Предмет дослідження – теоретичні засади, нормативно-правові механізми, практичні форми, методи та результативність реалізації державної політики щодо становлення і розвитку інформаційного суспільства в Україні.

Короткий зміст роботи. У роботі розкрито зміст поняття «інформаційне суспільство» та еволюцію концепцій його розвитку в державному управлінні. Проаналізовано нормативно-правове забезпечення та інституційну структуру реалізації цифрової політики в Україні, зокрема роль Міністерства цифрової трансформації. Досліджено практичні аспекти впровадження електронного урядування (e-government), цифровізації державних послуг (проєкт «Дія») та розбудови національної інфраструктури широкосмугового доступу до інтернету. Особливу увагу приділено проблемам інформаційної безпеки, подоланню цифрового розриву та забезпеченню стійкості інформаційного простору в умовах воєнного стану. Сформульовано рекомендації щодо гармонізації українського законодавства з цифровими стандартами ЄС.

Ключові слова: інформаційне суспільство, державна політика, цифровізація, електронне урядування, цифрова трансформація, інформаційна безпека, цифрова грамотність.

ABSTRACT

Pavliuk, Yu. Theoretical and Practical Aspects of State Policy in the Field of Information Society in Ukraine: qualification paper for the Master's degree; Speciality 281 "Public Management and Administration"; State University of Information and Communication Technologies; Research Supervisor O. A. Panchenko, Doctor of Science in Public Administration, Professor; Kyiv, 2025; 121 p.

The purpose of the qualification paper is a comprehensive study of the theoretical foundations of formation and an analysis of the practical aspects of implementing state policy in the sphere of the information society in Ukraine, as well as the development of scientifically grounded proposals and recommendations for its improvement, taking into account contemporary global challenges and European experience.

The object of the study is the state policy of Ukraine in the sphere of the information society and digitalization (including the development of e-government, ensuring cybersecurity, and bridging the digital divide).

The subject of the study is the theoretical foundations, regulatory and legal mechanisms, practical forms, methods, and the effectiveness of implementing state policy regarding the formation and development of the information society in Ukraine.

The thesis clarifies the concept of the "information society" and the evolution of its development concepts in public administration. The regulatory framework and institutional structure for digital policy implementation in Ukraine, specifically the role of the Ministry of Digital Transformation, are analyzed. Practical aspects of e-government implementation, digitalization of public services (the "Diia" project), and the development of national broadband infrastructure are investigated. Particular attention is paid to information security issues, bridging the digital divide, and ensuring the resilience of the information space under martial law. Recommendations for harmonizing Ukrainian legislation with EU digital standards are formulated.

Keywords: information society, state policy, digitalization, e-government, digital transformation, information security, digital literacy.

ЗМІСТ

ВСТУП **6**

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА ТА ДЕРЖАВНОЇ ПОЛІТИКИ У ЦІЙ СФЕРІ **13**

1.1. Еволюція концепцій інформаційного суспільства та його ключові характеристики. 13

1.2. Поняття, принципи та механізми державної політики у сфері інформаційного суспільства: вітчизняний та зарубіжний досвід. 20

1.3. Національні особливості та виклики формування інформаційного суспільства в Україні. 32

РОЗДІЛ 2. АНАЛІЗ СУЧАСНОГО СТАНУ ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ **41**

2.1. Законодавча та нормативно-правова база державної політики у сфері інформатизації та цифровізації в Україні. 41

2.2. Дослідження ключових напрямків державної політики. 51

2.3. Аналіз проблем та бар'єрів у реалізації державної політики у сфері інформаційного суспільства в Україні. 66

РОЗДІЛ 3. ШЛЯХИ УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ **78**

3.1. Стратегічні пріоритети та напрямки оптимізації державної політики у сфері інформаційного суспільства з урахуванням європейського досвіду. 78

3.2. Розроблення комплексу заходів щодо удосконалення державної політики у сфері інформаційного суспільства 86

3.3. Прогнозні оцінки та очікувані соціально-економічні ефекти від вдосконалення державної політики в інформаційній сфері. 97

ВИСНОВКИ **101**

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ **111**

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІКТ	- Інформаційно-комунікативні технології
ІС	- інформаційне суспільство
ІПСО	- Інформаційно-психологічні операції
CDO	- Chief Digital Officer – заступник з цифрової трансформації
GDPR	- захист даних
ЄС	- Європейський Союз
ШІ	- Штучний інтелект
КЕП	- електронний підпис
ЕУ	- Електронне урядування
ЦОВВ	- Центральні органи виконавчої влади
РНБО	- Рада національної безпеки і оборони України
ВПО	- Внутрішньо переміщені особи
НПА	- нормативно-правові акти
КІ	- критична інформаційна інфраструктура
ЦНАП	- Центр надання адміністративних послуг

ВСТУП

Актуальність теми. Важливість обраної проблематики диктується низкою вирішальних аспектів, що чинять прямий вплив на функціонування державного апарату, економічні показники та обороноздатність України у сучасному світовому контексті.

На цей час, прогрес України тісно сплетений із тенденціями становлення світового інформаційного суспільства та руху до Європейського Співтовариства. Наша держава обрала шлях узгодження вітчизняної політики у галузі інформаційно-комунікаційних технологій та електронних сервісів із правом та нормами ЄС, особливо з огляду на ініціативи «Digital Decade». Це, своєю чергою, накладає обов'язок провести детальне дослідження відповідності українських планів загальноєвропейським критеріям.

Застосування передових розробок, приміром, штучного інтелекту, масивів даних чи хмарних сервісів, постає не просто питанням економічної доцільності, а й імперативом політичним, щоби підтримати здатність країни конкурувати. У світовій інформаційній мережі, охорона державних цифрових активів та культурної спадщини набуває першочергового, стратегічного значення.

Значущість цього питання зростає завдяки вимогам, що висуваються як державним апаратом, так і громадами: насамперед, це стосується дієвості електронного урядування (е-врядування). Просування та інтеграція електронних сервісів (скажімо, через мобільний додаток «Дія») становить фундаментальний спосіб для посилення відкритості, мінімізації корупційних проявів і покращення взаємодії між пересічними громадянами або діловими колами та органами влади. Оцінка результативності цих інструментів є критично важливою; по-друге, це пов'язано з необхідністю зменшення нерівності у доступі до цифрових технологій. Нерівномірність у забезпеченні доступу до інформаційно-комунікаційних технологій та розбіжності у володінні цифровими навичками серед територій та різних прошарків

суспільства можуть підірвати соціальну згуртованість. Урядові стратегії мусять включати ефективні інструменти для подолання цієї ситуації.

В умовах військової агресії та гібридних загроз, в яких чинить опір держава, настанова політики щодо інформаційного суспільства набуває життєво важливого аспекту безпеки. Значущість цього питання зумовлена нагальною потребою безперервно вдосконалювати системи для захисту життєво важливої інфраструктури від кібернетичних посягань, протистояти кібератакам, а також гарантувати незмінну роботу державних інформаційних платформ. Державна політика повинна формувати дієві засоби для оборони вітчизняного інформаційного середовища від зовнішнього втручання та маніпулятивних впливів.

Таким чином, створення цілісного фундаменту теорії та надання практичних настанов для покращення державної стратегії у сфері інформаційного суспільства наразі є вчасною та життєво необхідною мірою для гарантування сталого прогресу, захисту національних інтересів та успішної євроінтеграції нашої держави.

Стан і ступінь розробки проблеми в спеціальній літературі

Проблема теоретичних і практичних аспектів державної політики у сфері інформаційного суспільства в Україні характеризується високим, але незавершеним ступенем розробки в спеціальній літературі. Дослідження мають міждисциплінарний характер, охоплюючи державне управління, політологію, право, економіку та інформаційні технології.

Теоретичні основи проблеми розроблені досить ґрунтовно як на міжнародному, так і на національному рівнях. Щодо міжнародної концептуалізації, то проблематика ґрунтується на класичних працях західних соціологів та економістів, таких як Деніел Белл (концепція постіндустріального суспільства), Манюель Кастельс (мережеве суспільство) та Елвін Тоффлер (третя хвиля). Ці роботи заклали основу для розуміння сутності інформаційного суспільства та суспільства знань.

Значний внесок зробили українські вчені, які адаптували ці концепції до національного контексту. Дослідження Г. Почепцова, О. Баранова, І. Жиляєва та О. Риженко зосереджені на теоретико-методологічних засадах інформаційної політики, електронного урядування та інформаційної безпеки.

Розробка правового та інституційного поля активно вивчається, але характеризується динамічністю та незавершеністю. Значна кількість праць присвячена аналізу законів України («Про електронні довірчі послуги», «Про хмарні послуги») та стратегічних документів (Стратегія цифрової трансформації). Дослідники вивчають відповідність цих актів стандартам ЄС (зокрема, регламентам eIDAS та директиві NIS. Особлива увага приділяється проблемам правових колізій, відсутності інтероперабельності державних реєстрів та інституційної спроможності органів влади для реалізації складних цифрових проєктів.

Аналіз практичної реалізації політики є найбільш проблемною та фрагментарною частиною розробки. Існує багато публіцистичних та аналітичних звітів про успіхи проєкту «Дія» та впровадження електронних послуг. Проте, не вистачає глибоких наукових емпіричних досліджень щодо реальної ефективності, якості та соціальної інклюзивності цих послуг. У зв'язку з військовою агресією з'явилася велика кількість досліджень, присвячених національній кіберстійкості, роботі Держспецзв'язку та протидії дезінформації. Цей напрямок є найбільш актуальним, але часто має описовий, а не глибоко аналітичний характер. Дослідження часто обмежуються аналізом даних про цифрову грамотність та доступ до Інтернету, але недостатньо розроблені дієві механізми для його подолання та оцінки соціально-економічних наслідків.

Таким чином, у спеціальній літературі проблема розроблена на теоретичному рівні, але існує науковий вакуум у сфері комплексного аналізу практичної ефективності державної політики, що постійно трансформується,

та розробки обґрунтованих прогностичних моделей її удосконалення. Це обґрунтовує актуальність і наукову новизну нашої магістерської роботи.

Зв'язок роботи з науковими програмами, планами, темами. Тема кваліфікаційної роботи пов'язана із виконанням завдань, передбачених стратегічними документами країни, зокрема з державними та національними програмами: Стратегією цифрової трансформації України, Національною стратегією у сфері кібербезпеки, Планами заходів щодо імплементації Угоди про асоціацію з ЄС.

Кваліфікаційне дослідження проводилося на кафедрі публічного управління та адміністрування Навчально-наукового інституту менеджменту та підприємництва Державного університету інформаційно-комунікаційних технологій і пов'язана з науково-дослідною темою кафедри «Теоретико-прикладні аспекти розвитку цифрової держави в Україні» (номер державної реєстрації 0123U102733).

Мета і завдання дослідження. Метою роботи є комплексне дослідження теоретичних засад формування та аналіз практичних аспектів реалізації державної політики у сфері інформаційного суспільства в Україні, а також розробка науково обґрунтованих пропозицій та рекомендацій щодо її удосконалення з урахуванням сучасних глобальних викликів та європейського досвіду.

Для досягнення поставленої мети необхідно вирішити наступні ***завдання*:**

1. Систематизувати та уточнити ключові теоретичні концепції, сутність та характеристики інформаційного суспільства та державної політики у цій сфері.
2. Проаналізувати та узагальнити зарубіжний досвід формування та реалізації державної політики у сфері цифровізації.

3. Дослідити еволюцію та поточний стан нормативно-правового та інституційного забезпечення державної політики у сфері інформаційного суспільства та цифровізації в Україні.

4. Провести комплексний аналіз практичної реалізації ключових напрямків державної політики, включаючи розвиток е-урядування, забезпечення кібербезпеки та подолання цифрового розриву.

5. Виявити основні проблеми, недоліки та бар'єри, що перешкоджають ефективній реалізації державної політики у сфері інформаційного суспільства в Україні.

6. Розробити конкретні науково-практичні рекомендації та обґрунтувати шляхи удосконалення державної політики з метою підвищення її ефективності та прискорення європейської інтеграції.

Об'єктом дослідження є державна політика України у сфері інформаційного суспільства та цифровізації (включаючи розвиток електронного урядування, забезпечення кібербезпеки та подолання цифрового розриву).

Предмет дослідження – теоретичні засади, нормативно-правові механізми, практичні форми, методи та результативність реалізації державної політики щодо становлення і розвитку інформаційного суспільства в Україні.

Методи дослідження. Для досягнення поставленої мети та завдань магістерської роботи використані наступні загальнонаукові та спеціальні методи дослідження: *метод аналізу та синтезу* застосовується для розчленування складної проблеми державної політики на окремі компоненти (е-урядування, кібербезпека, цифрова грамотність) та подальшого їх об'єднання для формування цілісного теоретичного погляду на інформаційне суспільство; *метод індукції та дедукції* – індукція використовується для узагальнення конкретних практичних випадків реалізації цифрових ініціатив (кейс-стаді) у формування загальних закономірностей, дедукція – для застосування теоретичних концепцій інформаційного суспільства до аналізу

політики України: *метод порівняння та аналогії* використовується для зіставлення вітчизняного досвіду реалізації державної політики з досвідом країн-лідерів (наприклад, Естонії, країн ЄС) з метою виявлення найкращих практик (best practices) та обґрунтування рекомендацій; *історико-логічний метод* дозволяє простежити еволюцію концепцій інформаційного суспільства та етапність розвитку державної політики у цій сфері в Україні від перших програм до сучасних стратегій цифровізації. Метод *контент-аналізу* застосовується для кількісного та якісного аналізу змісту великого масиву нормативно-правових актів (Закони, Стратегії, Концепції), офіційних звітів (Мінцифри, Держспецзв'язку), а також експертних та аналітичних матеріалів; за допомогою статистичного методу ми опрацювали кількісні дані з офіційних джерел (ООН E-Government Survey, індекси кібербезпеки, статистика використання електронних послуг) з метою об'єктивної оцінки ефективності політики. *Метод системного підходу* дозволив розглянути державну політику у сфері інформаційного суспільства як цілісну систему, що складається з взаємопов'язаних елементів (законодавство, інфраструктура, кадри, послуги), і виявляти системні проблеми; *метод моделювання та прогнозування* використаний для розробки практичних рекомендацій та обґрунтування очікуваних соціально-економічних ефектів від їх впровадження. Він дозволив змоделювати наслідки запропонованих змін у державній політиці.

Практичне значення одержаних результатів полягає у розробці науково обґрунтованих, системних та прикладних рекомендацій, які можуть бути безпосередньо використані для підвищення ефективності, прозорості та якості державної політики у сфері інформаційного суспільства в Україні. Сформовані пропозиції щодо оптимізації механізмів електронного урядування та підвищення кіберстійкості критичної інфраструктури мають пряму практичну цінність для посилення національної безпеки та зниження корупційних ризиків у державному секторі. Крім того, матеріали роботи можуть бути інтегровані в освітній процес при підготовці фахівців у галузі

публічного управління та інформаційної політики, а також слугувати об'єктивним інструментом оцінки для громадських організацій, які здійснюють моніторинг цифрової трансформації. Таким чином, одержані результати мають подвійне значення: вони підвищують якість теоретичного осмислення проблеми та надають конкретні інструменти для її практичного вирішення.

Апробація результатів роботи. Основні положення, висновки і рекомендації дослідження обговорювалися під час попереднього захисту кваліфікаційної роботи на засіданні кафедри публічного управління та адміністрування Навчально-наукового інституту менеджменту та підприємництва Державного університету інформаційно-комунікаційних технологій 19 грудня 2024 року; участь у II Всеукраїнській науково-практичній конференції «Теоретико-прикладні аспекти розвитку цифрової держави в Україні» 09 листопада 2024 року (доповідь з публікацією тез «Аналіз проблем та бар'єрів у реалізації державної політики у сфері інформаційного суспільства в Україні»).

Структура та обсяг кваліфікаційної роботи. Дослідження складається зі вступу, трьох розділів, висновків, списку використаних джерел. Повний обсяг кваліфікаційної роботи складає 121 сторінка. Список використаної літератури – 124 позиції.

Ключові слова: інформаційне суспільство, державна політика, цифровізація, електронне урядування, цифрова трансформація, інформаційна безпека, цифрова грамотність.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА ТА ДЕРЖАВНОЇ ПОЛІТИКИ У ЦІЙ СФЕРІ

1.1. Еволюція концепцій інформаційного суспільства та його ключові характеристики

Інформаційно-комунікаційні технології (ІКТ) є основним каталізатором та незамінною технологічною основою переходу від індустріального суспільства до інформаційного. Вони не лише прискорюють процеси, а й фундаментально змінюють економічні, соціальні та політичні взаємодії.

Інформаційне товариство (ІС) – це теоретична концепція та модель розвитку суспільства, в якій інформація, знання та інформаційно-комунікаційні технології (ІКТ) стають найважливішим економічним ресурсом, домінуючим фактором виробництва, центральним джерелом інновацій та визначальним елементом соціальної, політичної та культурної організації [13].

Характер ІС можна проілюструвати такими ключовими аспектами:

1. Знання та інформація, особливо теоретичні та кодифіковані знання, замінюють матеріальні ресурси та фізичну працю як головну рушійну силу економічного зростання та соціального розвитку.
2. Компанія спирається на розвинену інформаційну інфраструктуру (Інтернет, мережі, хмарні технології), що забезпечує швидкий, глобальний та масовий обмін даними.
3. Відбувається економічна трансформація: перехід від індустріального суспільства (виробництво товарів) до інформаційного чи суспільству знань (виробництво послуг, обробка даних, інновації).
4. Соціальні та економічні структури стають все більш мережевими та децентралізованими, що забезпечує гнучкість, але також посилює вплив глобальних потоків інформації та капіталу [18].

За своєю суттю інформаційне суспільство – це суспільство, в якому більшість громадян залучено до обробки, зберігання та передачі інформації та в якому доступ до цієї інформації та можливість її використання визначають соціальний статус та економічний успіх [97].

Концепція інформаційного суспільства виникла внаслідок тривалих соціологічних та філософських дискусій про глибокі потрясіння, викликані розвитком інформаційно-комунікаційних технологій (ІКТ). Розвиток цієї концепції та фактичне становлення інформаційного суспільства тісно пов'язані з технологічними революціями та пройшли через кілька важливих етапів [99].

1. Ранні концепції (1950-1960-ті роки)

До терміну «інформаційне суспільство» подібні ідеї описували перехід від індустріальної епохи:

- Концепція суспільства знань. Хоча цей термін часто використовується як синонім інформаційних систем, він з'явився набагато раніше. У 1950-х роках Пітер Друкер обговорював зростаючу важливість працівників, які мають знання, та знань як найважливішого економічного ресурсу.
- Теорія постіндустріального суспільства, ключова концепція, сформульована Денієлом Беллом у 1970-х роках, описує перехід від економіки, що виробляє товари, до економіки, орієнтованої на послуги, теоретичні знання та інформацію. Белл стверджував, що теоретичні знання стають основним джерелом інновацій та розробки політики. На відміну від індустріальної епохи, де основними ресурсами були капітал і праця, в постіндустріальну епоху ключовим ресурсом стають кодифіковані теоретичні знання. Науково-дослідні інститути, університети та спеціалізовані лабораторії стають майданчиками для знань, які потім безпосередньо застосовуються у виробництві та суспільстві [6].

Белл чітко окреслив перехід від економіки, заснованої на виробництві, до економіки, що базується на знаннях та послугах. Він був першим, хто підкреслив, що теоретичні знання є основною рушійною силою змін, задовго до поширення інтернету. Його робота заклала концептуальну основу для аналізу трансформацій у сфері зайнятості та владних структур [88].

Незважаючи на деяку критику, концепція Белла мала значний вплив. Зокрема, Кастельс розвинув її далі, змістивши акцент із простою заміною «товарів» на «послуги» на мережеву структуру та інформаційні потоки, що стали можливими завдяки мікроелектроніці [30].

2. Виникнення концепції інформаційного суспільства (1970-1980-ті рр.)

Термін «інформаційне суспільство» (яп. jōhōka shakai) вперше з'явився в Японії наприкінці 1960-х – на початку 1970-х років [114].

- Японська школа (Йонедзі Масуда, Тадао Умесао) зосередилася на комп'ютеризації та розвитку інформаційної інфраструктури. У своїй роботі 1980 році «Інформаційне суспільство як постіндустріальне суспільство» Масуда виклав концепцію суспільства, процвітання якого засноване на цінності інформації, а не матеріальних благах [114].
- Західна школа (Марк Порат, Фріц Махлуп) зосередилася на економічних показниках та проаналізувала частку інформаційного сектора у національному ВВП, а також зростання кількості людей, зайнятих у сфері обробки інформації [115].

3. Глобалізація та мережеве суспільство (1990-ті роки – початок XXI століття)

Зі зростанням поширення Інтернету та глобалізацією концепція інформаційних систем набула нового, взаємопов'язаного виміру.

Мануель Кастельс став провідним теоретиком цієї доби. Він стверджує, що важлива відмінність сучасності полягає у обсязі інформації, а й у структурі суспільства: мережа стає домінуючою формою соціально-економічної організації, замінюючи традиційні ієрархічні і вертикальні структури. Мережі

гнучкі, децентралізовані та самоперебудовуються. Вони можуть розширюватися або скорочуватися при необхідності, а також додавати або видаляти вузли. Суспільство організоване навколо потоків – потоків інформації, капіталу, технологій, зображень та організаційних взаємодій, які циркулюють глобально та практично в реальному часі. Той, хто контролює ці потоки, має реальну владу. «Простір потоків» відноситься до фізичної, електронної та організаційної інфраструктури, що забезпечує глобальний рух цих потоків. Цей простір контрастує із «простором місць» – традиційною, географічно визначеною локальною соціальною організацією. У мережевому суспільстві «простір потоків» домінує над «простором місць» [30].

Кастельс визначає інформаціоналізм як нову технологічну парадигму, яка прийшла на зміну індустріалізму. У той час як остання ґрунтувалася на енергії, інформаціоналізм спирається на технології виробництва, обробки та символічної передачі знань. Продуктивність залежить від інновацій та адаптивності. На відміну від попередніх технологічних революцій (наприклад, промислової революції), де технології впливали на матерію, в інформаціоналізмі вони впливають на інформацію. Це призводить до безперервного зворотного зв'язку, в якому інформація є як входом, так і виходом [30].

Інформаційні мережі та глобалізація трансформують індивідуальну та колективну ідентичність. Зіткнувшись із дестабілізуючою силою глобальних мереж, люди шукають притулку у первинних ідентичностях (релігійних, національних, етнічних, територіальних) і знаходять у них сенс свого існування. Ці ідентичності стають «ідентичностями опору» в анонімній логіці мереж. Таким чином, суспільство розколюється на універсальні, глобальні мережі та специфічні локальні ідентичності.

Кастельс описує формування глобальної еліти, що працює в «просторі потоків» (менеджери з інформації, фінансисти), і зростаючу групу

виключених або взаємозамінних працівників, чию роботу можна легко автоматизувати або передати на аутсорсинг до інших регіонів.

Кастельс також використовує термін «четвертий світ» для позначення груп населення, маргіналізованих або виключених із глобальної системи. Сюди входять як бідні країни, а й соціально виключені групи населення у промислово розвинених країн: бездомні, безробітні, ув'язнені і маргіналізовані етнічні групи. Вони не просто «відсталі» у своєму розвитку, а й структурно відрізані від механізмів створення вартості та виробництва влади у мережевому суспільстві [30].

Внесок Кастельса є фундаментальним, оскільки він розширив рамки аналізу, вивівши його за рамки технологій. Він продемонстрував, що, хоча інформаційно-комунікаційні технології (ІКТ) є необхідною умовою змін, вони не є єдиною: вони взаємодіють із капіталізмом, державою та культурою. Він розробив структурну модель. Його концепції «простору потоку» та «мережевої логіки» надали соціології необхідні інструменти для аналізу нової просторово-часової організації. Він виділив конфлікти і підкреслив напругу між глобальними мережами (інструментальна раціональність) та локальними ідентичностями (пошук сенсу), а також зростаючу соціальну нерівність, що виникає внаслідок цього структурного розриву [30]. По суті Кастельс розробив теорію соціальної структури для епохи Інтернету, що зробило його роботу незамінною для розуміння інформаційного суспільства.

На цьому етапі основна увага приділяється економіці, яка базується на знаннях, де найважливішим джерелом конкурентної переваги є здатність впроваджувати інновації, швидко вчитися та керувати інформацією.

4. Сучасні концепції та виклики (21 століття)

Все більшого поширення набувають мобільні пристрої, соціальні мережі, розвиток штучного інтелекту (ШІ), Інтернету речей (IoT), великих даних та хмарних обчислень.

Головний аспект стосується «суспільства знань». Акцент зміщується з технологій (які просто надають інформацію) на здатність суспільства використовувати знання для вирішення соціальних та економічних проблем.

Було створено концепцію «Суспільство 5.0» (Японія), в якій інтеграція кіберпростору та фізичного простору спрямована на досягнення сталого та надрозумного суспільства. На суспільному рівні ми живемо в епоху постійної мережевої взаємодії, цифрової трансформації всіх секторів економіки та зростання загроз, пов'язаних із кібербезпекою, фейковими новинами та витоками даних [85].

Зріле інформаційне суспільство характеризується як наявністю технологій, так і їх глибокою інтеграцією в соціальну мережу. Значна частка працюючого населення (понад 50%) залучена в обробку та створення інформації. Відбувається глобалізація комунікацій, де інформація передається в режимі реального часу глобальними мережами, долаючи національні та географічні кордони. Високий рівень цифрової грамотності дозволяє значній частині населення освоювати цифрові технології та критично оцінювати інформацію [85].

В галузі електронного уряду та демократії використання інформаційно-комунікаційних технологій є важливим для підвищення прозорості та ефективності державного управління, а також для залучення громадян до політичних процесів. Домінує інтелектуальна власність, а захист та торгівля правами на інтелектуальну власність (патенти, авторські права) стають вирішальними для економіки [98].

Інформаційне суспільство має низку фундаментальних характеристик, які відрізняють його від індустріального суспільства [98]:

1) Сфера економіки:

а) домінування інформаційного сектора – найбільша частина ВВП створюється у сфері послуг, пов'язаних з інформацією, знаннями та комунікацією;

б) знання як найважливіший ресурс – інтелектуальний капітал (кваліфікація, освіта, інновації) стають цінішими, ніж матеріальний капітал;

в) автоматизація та гнучкість виробництва. Виробництво стає високотехнологічним, гнучким та адаптованим до індивідуальних потреб.

2. Технологічна сфера:

а) інформаційно-комунікаційні технології (комп'ютери, інтернет, мобільний зв'язок) проникають у всі сфери життя – від роботи та освіти до побуту та дозвілля;

б) поєднання різних технологій (ЗМІ, телекомунікації, комп'ютери) у єдину цифрову інфраструктуру;

в) розвиток глобальних високошвидкісних мереж (наприклад, 5G, оптоволоконні мережі).

3. Соціальна сфера:

а) соціальні та економічні взаємодії відбуваються у горизонтальних та динамічних мережах (організаціях, соціальних мережах), які є більш гнучкими, ніж традиційні ієрархії;

б) потоки інформації, капіталу та культурні стають транснаціональними та утворюють глобальне інформаційне середовище;

в) поширення віддаленої роботи, самозайнятості та зростаюча потреба у кваліфікованих працівниках.

4. Культурна сфера:

а) інформаційне навантаження. Обсяг доступної інформації зростає експоненційно, вимагаючи нових навичок її фільтрації та критичної оцінки;

б) більшість соціальних та політичних подій опосередковуються цифровими ЗМІ;

в) користувачі стають не лише споживачами, а й творцями контенту (блоги, відео, соціальні мережі), цим зруйнувавши монополію традиційних ЗМІ.

Такий розвиток від постіндустріальної епохи через мережеву епоху до «Суспільства 5.0» показує, що інформаційне суспільство – це не кінцева точка, а безперервний і динамічний процес, який постійно змінює економіку, політику та соціальні відносини [98].

Таким чином, інформаційно-комунікаційні технології (ІКТ) є основним чинником сучасності та докорінно змінюють характер людської діяльності. Їхня роль полягає у забезпеченні інформаційнізму (згідно з Кастельсом) [30] – режиму розвитку, в якому основним джерелом продуктивності та влади є технології генерації, обробки та передачі інформації.

1.2. Поняття, принципи та механізми державної політики у сфері інформаційного суспільства: вітчизняний та зарубіжний досвід

Державне регулювання у сфері інформаційного соціуму являє собою планомірну, упорядковану діяльність владних інституцій та управлінських структур, яка реалізується у співпраці з елементами громадянського суспільства та комерційними суб'єктами. Метою цього процесу є напрацювання законодавчих, фінансових, суспільних, структурних та технічних передумов для плідного становлення та прогресу інформаційно орієнтованого співтовариства [68].

Фундаментальне значення цієї стратегії полягає не лише в оснащенні державних установ комп'ютерною технікою, а й у кардинальній перебудові усіх аспектів життя суспільства (економіки, адміністрування, навчання, культури) завдяки масовому впровадженню інформаційно-комунікаційних засобів .

Складовими ключовими поняттями у цій сфері виступають:

а) ті, хто формує політику: найвищі державні інституції (Законодавчий орган, Президент, Уряд), профільні відомства (в Україні це насамперед Міністерство цифрової трансформації), органи місцевого самоврядування, а

також об'єднання підприємців та громадянські ініціативи, що виступають у ролі спільних учасників [27] ;

б) те, на що спрямована політика: взаємозв'язки у сфері інформації, технічна база інформаційно-комунікаційних технологій, цифрові права населення, національні інформаційні фонди, поле розгортання електронних сервісів.

Ключовим завданням у цій сфері є покращення рівня життя населення, гарантування здатності вітчизняної економіки конкурувати на глобальній арені, оптимізація роботи урядових структур та зміцнення обороноздатності країни за допомогою застосування цифрових засобів.

Ця політика має вирішальне значення, оскільки вона формує позицію держави у нинішньому цифровому вимірі: чи стане вона генератором інновацій та інтелектуального капіталу, чи лише споживачем наявних рішень; а також чи зможе забезпечити самостійність у сфері інформаційного простору.

Щодо принципів державної політики у царині інформаційного суспільства, то ними є фундаментальні засади та керуючі ідеології, на яких ґрунтується уся діяльність держави у межах цієї сфери. Вони гарантують моральність, результативність та передбачуваність такої політики [27].

Основними критеріями принципів виступають:

1. Людиноцентризм та верховенство людських прав. Розвиток інформаційного суспільства повинен насамперед приносити користь людині. Жодні технологічні впровадження не мають ставати причиною порушення фундаментальних прав, таких як право на приватність, вільне висловлювання думок чи доступ до знань. Технології мусять бути інструментом на службі людини, а не навпаки [21].

2. Прозорість та загальна доступність (подолання цифрової нерівності). Необхідно гарантувати однаковий доступ до інформаційних ресурсів, інформаційно-комунікаційних технологій та електронних сервісів для усіх громадян, без огляду на те, де вони мешкають (місто чи сільська місцевість),

їхній вік, соціальне становище чи фізичні обмеження. Це охоплює як фізичну можливість підключення до мережі, так і володіння необхідними цифровими компетенціями.

3. Інформаційна безпека та кіберзахист. Жоден розвиток у напрямі інформаційного суспільства не зможе відбутися, якщо не будуть забезпечені належні гарантії щодо захисту даних – чи то особистої інформації, чи то державних реєстрів. Сюди ж входить охорона життєво важливих об'єктів інфраструктури від ворожих кібернападів та протидія поширенню неправдивих відомостей [70].

4. Верховенство права у цифровому просторі: як і у звичному світі, право має встановлювати правила для взаємодії в мережі та у цифровій сфері. Це поширюється на укладання електронних угод, захист прав на інтелектуальну власність та притягнення до відповідальності за злочини в кіберпросторі.

5. Інноваційність та технологічна нейтральність. У цьому сенсі органи влади повинні заохочувати застосування найсучасніших технологічних рішень (штучний інтелект, блокчейн, інтернет речей), водночас правова база зобов'язана уникати необґрунтованого фаворитизму щодо будь-якої окремої технології, даючи змогу ринковим механізмам визначати найбільш дієві варіанти.

6. Співпраця на засадах партнерства. З огляду на те, що органи влади не спроможні самостійно збудувати інформаційне суспільство, їм життєво необхідний безперервний обмін думками та спільна робота з представниками ІТ-сектору, науковими колами, освітніми закладами та громадськими діячами.

7. Приєднання до глобального інформаційного простору. Необхідно синхронізувати державні стандарти з тими, що діють на міжнародному рівні (насамперед, європейськими), та гарантувати можливість взаємодії електронних сервісів між країнами (як приклад, спільне визнання електронних підписів з Європейським Союзом).

Створення державної стратегії щодо інформаційного суспільства потребує не лише базових юридичних та інституційних структур, а й таких, що є адаптованими та гнучкими. Часто, усталені методи не в змозі встигати за швидкістю технологічного розвитку, що спричиняє необхідність у розробці оновленого законодавства, яке б урегульовувало нові цифрові взаємини; створення профільних органів, що здатні осягнути та відповідати на виклики цифрової ери; а також у залученні до міжнародної взаємодії, зважаючи на те, що «цифрові кордони» не мають чітких меж.

Інструментарій, важелі та методи, якими держава втілює у життя вже згадані засади та доходить до визначених цілей, називаються механізмами. Класифікувати їх можна за типом їхнього впливу.

Механізми – це інструментарій, важелі та способи, за допомогою яких держава втілює вищезгадані принципи в життя та досягає поставлених цілей. Їх можна згрупувати за характером впливу [81].

1. Нормативно-правові механізми. Це основа будь-якої політики – формування нормативно-правового поля, що узаконює цифрові процеси. До таких належить ухвалення законодавчих актів щодо електронних довірчих послуг (включно з електронним підписом), захист особистих даних, хмарні рішення, а також забезпечення доступу до загальнодоступної інформації. Сюди ж належить створення національних стратегій та концепцій (стратегія розвитку електронної економіки та цифрового суспільства України).

2. Структурно-інституційні засади – формування апарату влади, якому доручено цифровізаційні процеси та чітке окреслення сфери їхньої компетенції. Приміром, діяльність профільних відомств (як-от Міністерство цифровізації), впровадження посад CDO (Chief Digital Officer – заступників, відповідальних за цифрові зміни) у кожному міністерстві та на рівні регіональних управлінь. Заснування профільних установ для забезпечення кібербезпеки (скажімо, Державна служба спеціального зв'язку та захисту інформації, Кіберполіція).

3. У сфері фінансів та економіки, механізми, що є рушійною силою, відповідають за забезпечення необхідними ресурсами та формування системи економічних заохочень. Сюди належить спрямування бюджетних коштів на фінансування програм, пов'язаних із впровадженням інформаційних технологій, а також проведення державних закупівель послуг у сфері IT, що слугує потужним стимулом для розвитку ринку. Окрім того, важливими є запровадження особливих податкових умов для IT-підприємств (як от український проєкт «Дія.City»), надання фінансової підтримки (грантів) для початківців у бізнесі (стартапів), а також залучення капіталу з-за кордону для модернізації цифрової інфраструктури [27].

4. Техніко-технологічні механізми являють собою безпосереднє формування як програмних платформ, так і необхідної інфраструктури. До цього спектру входять: а) електронне урядування (розробка порталів для надання публічних сервісів, приміром, «Дія», а також запровадження систем електронного документообігу у державних установах); б) інфраструктурні об'єкти: розвиток широкосмугових інтернет-мереж (з акцентом на сільські території), організація національних дата-центрів, впровадження сучасних стандартів зв'язку, як-от 4G та 5G; в) політика відкритих даних (забезпечення функціонування платформ, де державна інформація стає доступною у форматі, придатному для машинного опрацювання, з метою вільного використання її комерційними структурами та громадянами).

5. Механізми, пов'язані з персоналом та освітньо-культурною сферою, є ключовими для нарощування людського капіталу, адже без нього будь-які технології залишаються нежиттєздатними. До таких заходів, зокрема, належить запуск ініціатив щодо підвищення рівня цифрової обізнаності серед громадян (як-от «Дія.Цифрова освіта»), оновлення програм підготовки в галузі інформаційних технологій у вищих навчальних закладах, створення курсів для перепідготовки державних службовців, а також активне просування культури користування цифровими інструментами та правил безпеки у мережі [94].

Державна політика у сфері національної інформаційної спільноти являє собою складну багатошарову структуру. Вона об'єднує стратегічні накреслення (основи та вектори спрямування) із засадами моралі (норми) та арсеналом практичних засобів (важелі впливу). Ефективність даної політики зумовлена злагодженістю усіх важелів дії: неможливо спорудити цифрову державу виключно через ухвалення законодавчих актів, якщо відсутнє мережеве сполучення або громадяни не володіють навичками його використання [28].

У нинішньому ландшафті інформаційного суспільства, нам необхідно залучати передові міжнародні практики, адже жодна держава не володіє ексклюзивним правом на винахід інноваційних та дієвих підходів.

Ознайомлення із практиками, напрацьованими за кордоном, дає змогу не витрачати час на створення вже відомого – а саме, впроваджувати випробувані методи та дієві напрацювання; передбачати труднощі, бо знання про досвід інших держав забезпечує кращу готовність до можливих негараздів; впроваджувати передовий досвід – не сліпо передрук, а винахідливе припасування моделей до вітчизняних реалій; порівняти різноманітні шляхи, щоб чітко бачити, які саме стратегії продемонстрували більшу чи меншу ефективність у різних умовах. У підсумку, майже усі країни, незалежно від їхнього економічного рівня, розглядають інформаційне суспільство як вирішальний чинник для зростання конкурентоспроможності та загального добробуту [7].

Міжнародна практика впровадження державної політики у царині інформаційного суспільства являє собою розмаїття підходів: від ринково-орієнтованого й вільного (як у Сполучених Штатах) до суспільно-спрямованого, де держава відіграє провідну роль у гарантуванні доступу та розвитку цифрових навичок (типово для держав Євросоюзу та Скандинавії). Вивчення цих практик має першочергове значення для осмислення ефективних шляхів цифровізації, особливо стосовно гарантування рівного

доступу та захисту інформації, допомагає оминати усталені прорахунки та значно стимулювати внутрішні процеси переходу до цифри. Зокрема, закордонні напрацювання є визначальними у таких площинах:

1. Формування державних програм розвитку. Закордонний досвід, як от приклад електронного урядування в Естонії чи підходи до цифрової інтеграції у скандинавських державах, наочно показує методики досягнення значних успіхів у сфері надання цифрових сервісів та активізації участі населення, водночас суттєво спрощуючи адміністративні процеси. Це дає змогу нам обирати вже випробувані та найбільш дієві напрямки для нашого прогресу, замість того, аби витрачати ресурси на розробку власних рішень з нуля [93].

2. Охорона кіберпростору. Здатність протистояти кібернетичним викликам, впровадження нормативів щодо обробки особистої інформації (як-от GDPR у Євросоюзі) та формування надійної захищеності життєво важливих IT-систем являють собою надзвичайно важливий елемент для гарантування безпеки держави в епоху посиленої цифрової залежності [117].

3. Сприяння інноваційним процесам та економічному піднесенню. Передовий досвід, набутий у сферах підтримки стартапів, розвитку цифрових формацій господарства та залучення капіталовкладень у передові технологічні галузі (зокрема, зразки Ізраїлю та Сінгапуру), цілком можливо адаптувати з метою посилення світової конкурентоспроможності нашої країни.

Отже, залучення міжнародної практики стає життєво важливим кроком на шляху до формування в Україні інформаційного суспільства, що характеризується зрілістю, надійністю та відкритою інклюзивністю.

Світова практика впровадження державою політики у сфері інформаційного суспільства вирізняється великою варіативністю. Це зумовлено тим, що кожна держава підлаштовує загальносвітові тренди під власні особливі культурні, економічні, політичні та технологічні реалії. При цьому можна виявити спільні аспекти, проблеми та вдалі приклади, які можуть стати важливим джерелом знань.

Наведемо основні схеми та методи, які застосовувалися у цій сфері за кордоном. Тут можна окреслити декілька основних моделей, хоча насправді держави нерідко комбінують риси із різних концепцій:

1. *Скандинавська модель* (Данія, Швеція, Фінляндія, Естонія). Основною рисою подібної моделі слугує значний рівень поширення доступу до мережі, жваве впровадження системи електронного урядування (e-government) разом із наданням електронних сервісів (e-services), відкритість діяльності, певна ступінь довіри громадян як самим технологіям, так і державним інституціям, рішучий пріоритет, наданий кіберзахисту та охороні інформації, а також помітний рівень володіння цифровими навичками серед населення. Серед визначальних елементів варто виділити запровадження «Цифрового посвідчення особи» для громадян (приміром, Mobile-ID, як це реалізовано в Естонії), можливість електронного волевиявлення, повне переведення адміністративних послуг у цифрову форму, активне застосування уніфікованих ідентифікаторів та акцент на співпраці між державою та приватним сектором. Естонію нерідко іменують «цифровим тигром» завдяки її вражаючому темпу цифровізації [93].

Ключовими чинниками, що відіграють тут визначальну роль, є рівень довіри, відкритість інформації, вкладення коштів у розвиток цифрової інфраструктури та освітніх програм, а також відкритість до інноваційних підходів, що є вирішальними для досягнення успіху.

2. *Англосаксонська модель* (Велика Британія, США, Канада, Австралія). Примітно, що значна роль у поступі інформаційно-комунікаційних технологій відводиться ринковим механізмам та приватним підприємствам. Держава, зі свого боку, зосереджує зусилля на формуванні сприятливих регуляторних умов, стимулюванні інноваційної діяльності та посиленні конкурентного середовища [108]. Особлива увага приділяється концепції відкритих даних (Open Data) та досягненню прозорості в діяльності державних органів. Характерними елементами цієї парадигми є розвиток мереж стартапів,

залучення венчурного капіталу, а також державна фінансова підтримка науково-дослідних та дослідно-конструкторських робіт. У Великій Британії було започатковано практику «цифрових урядів» для забезпечення єдиного підходу до запровадження стандартів електронних сервісів [111]. Ключовими висновками для формування інформаційного суспільства слугують цінність конкуренції, необхідність постійних інновацій та здатність влади до оперативного реагування на технологічні трансформації.

3. *Азійська модель (Південна Корея, Сінгапур, Японія, Китай)*.

У державах подібного типу ми часто спостерігаємо вагоме державне управління та далекоглядне стратегічне бачення, що гармонійно поєднується з динамічними змінами у сфері технологій. Це проявляється у значних інвестиціях у ключові елементи інфраструктури (наприклад, високошвидкісний доступ до мережі), акцентуванні уваги на інноваційних розробках та спрямуванні зусиль на нарощування експорту інформаційно-технологічних послуг.

Південна Корея яскравий приклад: вона утримує світові позиції за показниками швидкості мережевого з'єднання та поширеності мобільних рішень. Уряд країни рішуче підтримує IT-сферу, виділяючи значні кошти на науково-дослідні та дослідно-конструкторські роботи [113]. Тим часом, Сінгапур реалізує програму «Smart Nation», де уряд бере на себе роль архітектора, проектуючи майбутнє, що передбачає всебічну інтеграцію передових технологій в усі сфери (від логістики та медичного обслуговування до системи освіти). Китай демонструє велику державну політику розвитку IT-сектору, надаючи допомогу своїм технологічним лідерам, водночас ретельно регулюючи інформаційне середовище (що відображається у функціонуванні механізму цензури, відомого як «Велика китайська стіна») [52].

4. *Країни ЄС (як єдиний простір)*.

Притаманні цій моделі знакові риси – це уніфіковані законодавчі основи (зокрема, щодо захисту персональних даних, як-от GDPR), розпорядження про

електронну ідентифікацію та плани розвитку єдиного цифрового ринку. Усі вони спрямовані на ліквідацію перешкод для транскордонної електронної комерції та надання послуг між державами-учасницями [117]. Першорядне значення надається гарантуванню прав кінцевих користувачів, безпеці цифрових мереж та узгодженню технічних норм. Активно заохочуються заходи, спрямовані на підвищення рівня цифрових навичок населення, допомога новоствореним європейським бізнесам (стартапам), а також доктрина спільного нормативного регулювання та міжнародної взаємодії з метою формування спільного цифрового середовища.

Основні механізми, за якими впроваджується ця політика в перелічених державах, охоплюють:

1. Електронний уряд.

В Естонії перевагою є те, що майже 99 % державних послуг надаються в електронному форматі, включно з інститутом електронного громадянства [93]. Данія ж запровадила для своїх громадян обов'язкове використання цифрової пошти для всієї офіційної комунікації з державними установами. Тим часом Канада оперує комплексною ініціативою «Government of Canada Digital», яка слугує хабом для централізованого контролю над цифровими державними сервісами.

Ці ключові аспекти демонструють яскравий приклад ефективності, виміряної у скороченні часу очікування в чергах, зростанні відкритості процесів та мінімізації корупційних ризиків.

2. Цифрова економіка та інновації.

Основоположною галуззю Ізраїлю є концепція «Старт-нація», що стала можливою завдяки державним стимулам, залученню фінансування та сприятливим умовам для ведення бізнесу [82].

У Сполучених Штатах світове лідерство в інформаційних технологіях обумовлене потужною інноваційною мережею (на кшталт Кремнієвої долини),

наявністю значних венчурних ресурсів та високим рівнем академічних розробок.

3. Кібербезпека.

На території Німеччини налагоджена ґрунтовна система заходів кіберзахисту, ключовим елементом якої є Федеральне відомство з безпеки інформаційних технологій (BSI). В Америці ж функціонує розгалужена мережа кіберзахисту, де залучені як державні органи (зокрема NSA та Міністерство внутрішньої безпеки), так і приватний сектор. Подібна взаємодія забезпечує ефективне планування, спрямування коштів на інноваційні засоби захисту та активну участь у міжнародному обміні досвідом [104].

4.Подолання цифрової нерівності:

Південна Корея приділяє значну увагу впровадженню розгорнутих освітніх кампаній для навчання громадян похилого віку навичкам користування мережею. Натомість, Індія реалізує ініціативу під назвою «Цифрова Індія», скеровану на забезпечення доступу до мережі у віддалених сільських місцевостях та нарощування цифрових компетенцій населення. Варто відзначити позитивний аспект, що полягає у функціонуванні спеціальних проєктів для тих верств населення, які перебувають у вразливому становищі, а також у спрямуванні коштів на розвиток необхідної інфраструктури у географічно ізольованих територіях [107].

5.Захист даних та приватність.

У державах Європейського Союзу запроваджено завищені вимоги щодо охорони персональних даних, які слугують зразком для багатьох націй. Закони функціонують прозоро, висуваються жорсткі критерії до суб'єктів, що опрацьовують дані, а також закріплено право громадян на володіння контролем над власною інформацією [117].

Проте, існує ряд викликів, які постають перед державами. Насамперед, це кібернетичні небезпеки. Ми бачимо наростання кібератак, поширення неправдивої інформації та поєднання різних гібридних загроз [28]. Другий

аспект — захист приватності: доводиться врівноважувати прагнення до інновацій, потреби у безпеці та збереження особистих даних. По-третє, йдеться про нерівність у доступі до цифрового світу. Критично важливо гарантувати усім громадянам однакову можливість користуватися технологіями та набувати цифрових умінь [15]. Четвертий пункт стосується етичних дилем, пов'язаних із Штучним Інтелектом. Постає потреба у створенні етичних настанов для ШІ та інших передових розробок. П'яте — ускладнення узгодження політик на світовій арені, що стосується гармонізації регулювання. Шосте — інертність бюрократичних структур. Маємо справу з протидією оновленням з боку усталених державних інституцій. І, нарешті, сьоме — потреба у фінансуванні: потрібні суттєві вливання коштів у цифрову основу та сервіси [2].

Таким чином, зарубіжний досвід свідчить: для ефективної державної політики у царині цифрового суспільства потрібна прозора та чітка концепція розвитку та провідна роль, рішучість політичних діячів та ухвалені на найвищому рівні національні плани дій.

Необхідною умовою є спрямування значних коштів на розвиток цифрової інфраструктури, освітніх програм та заходів із захисту кіберпростору. Державні послуги повинні бути максимально комфортними у користуванні, мати широкий доступ та високий рівень захищеності для усіх мешканців [110]. Основою успіху є прозорість та конструктивна взаємодія, що передбачає активне включення бізнесу, науковців та громадських організацій. Що стосується гнучкості, то держава має демонструвати здатність миттєво реагувати на новітні технологічні досягнення та виклики. Врешті-решт, міжнародна взаємодія повинна ґрунтуватися на узгодженні норм та регламентів, а також на регулярному обміні набутим досвідом.

Кожна держава мусить спершу визначити власний шлях, проте здатність оминати типові прорахунки та значно пришвидшити прогрес досягається

через скрупульозне дослідження й імплементацію передових здобутків світових флагманів у зведенні цифрового суспільства [77].

1.3. Національні особливості та виклики формування інформаційного суспільства в Україні

У сучасну еру домінуючим елементом усіх різновидів протистоянь виступає інформаційне протистояння. Наразі жоден збройний міжнародний конфлікт не обходиться без залучення інструментів інформаційного тиску, зокрема, інформаційних технологій. Внаслідок цієї ситуації, коли суб'єкти міжнародних відносин виявляються вразливими та недостатньо захищеними, що спричиняє системну кризу у сфері міжнародної інформаційної безпеки, створюються умови для подальшого формування інформаційного суспільства [50].

З огляду на це, критично важливим є питання формування такого суспільства, яке б базувалося на практичних механізмах, сумісних із міжнародними стандартами інформаційної безпеки. Це має гарантувати результативну інформаційну комунікацію між індивідами, їхній безперешкодний доступ до глобальних інформаційних надбань та задоволення їхніх запитів. Гарантом виконання цього завдання мають виступати міжнародні органи, спроможні забезпечити всебічне врегулювання політичного аспекту інформаційної безпеки, при цьому максимально залучаючи до процесу та враховуючи позиції й інтереси всіх держав світу .

Нинішні проблеми та небезпеки спричинили необхідність перегляду як теоретичних положень, так і практичних засад міжнародної взаємодії, а також внутрішньої політики, коли йдеться про гарантування кіберзахищеності в інформаційному суспільстві [43]. Адже, для підтримки сталості та захищеності у світі сьогодні необхідно ухвалити спільні настанови, засади та стандарти підзвітності.

У «Женевській Декларації принципів» наголошується на потребі здолати розрив у використанні цифрових технологій між державами та гарантувати доступ до цифрових благ усім країнам. Це має на увазі рівноправний, справедливий та безперешкодний доступ до ІКТ (інформаційно-комунікаційних технологій), їхніх сервісів та необхідної інфраструктури [105]. «Женевський план дій» передбачає формування інформаційного суспільства у всіх його вимірах: на світовому, державному та міжрегіональному рівнях.

Як європейська країна, Україна не цурається сучасних викликів глобалізації, а навпаки, долучається до творення інформаційного суспільства майбутнього. Вона вже зараз висуває ідеї стосовно забезпечення безпеки, закріплені у Київському безпековому договорі. З іншого боку, філософська думка має на меті осягнути цю політичну лінію у ширшому світоглядному сенсі – як певну національну мету або ідею, що постає на тлі епохи протистояння ідентичностей та так званого «зіткнення цивілізацій» (концепція С. Хантінгтона) [92].

Трансформація України у напрямку інформаційного суспільства (ІС) являє собою багатогранний та тривалий процес. Як ми вже констатували раніше, для ефективної реалізації цього розриву критично важливо залучати світові напрацювання у сфері становлення ІС та керування національними інформаційними процесами. Застосування найкращих методик та запроваджених рішень, які довели свою дієвість в інших державах, прискорить адаптацію до вітчизняних реалій, з огляду на особливості національного менталітету та поточні економічні обставини.

Курс на становлення інформаційного суспільства в Україні обрано визнаним стратегічним напрямком, що вимагає всебічного впровадження інформаційно-комунікаційних технологій (ІКТ) у кожну сферу життєдіяльності: починаючи від державного управління (електронне урядування) та комерційної діяльності (електронна торгівля), аж до освітнього

процесу, системи охорони здоров'я, і щоденної взаємодії між громадянами. Проте, ця трансформація несе із собою низку суттєвих специфічних рис та перешкод, серед яких головними та найважливішими стоять питання інформаційної захищеності та посилення кібернетичних ризиків.

Кібербезпекові питання та загрози у цифровій сфері, без сумніву, постають як найбільш нагальна проблема. Наша держава, Україна, неухильно зазнає інтенсивних кібератак та інформаційних втручань, що походять від держави-агресора [73]. У зв'язку з цим, першочерговими цілями визнано гарантування захисту життєво важливих об'єктів інфраструктури, збереження державних інформаційних ресурсів та ефективна протидія дезінформаційним кампаніям.

Кіберзагрози, що постають перед Україною, вирізняються унікальною особливістю. Вони часто зумовлені гібридною агресією та тривалим геополітичним протистоянням, що, своєю чергою, підвищує їхню потужність та руйнівний потенціал у зіставленні з багатьма іншими державами. Насамперед, тут ідеться про небезпеку для обороноздатності країни та життєво важливих об'єктів. Кібератаки цілять у стратегічні системи (енергопостачання, логістика, фінансовий сектор, зв'язок), аби дестабілізувати функціонування урядових структур та створити суспільну паніку. У результаті вдалих атак виникають значні фінансові втрати, припиняється постачання необхідних послуг (перебої з електропостачанням), а також руйнується віра громадян у державні інститути.

По-друге, спостерігається зневіра у цифрові послуги. Регулярні та вдалі кібератаки, витік особистої інформації або ж спотворення даних (неправдиві новини, дезінформаційні кампанії) руйнують віру населення в електронні послуги (на кшталт «Дії», електронних баз даних) та інформаційно-комунікаційні технології загалом. Це, в своєю чергою, має негативні наслідки, адже уповільнює процес переходу до електронного урядування та слугує перешкодою для цифровізації, оскільки громадяни ухиляються від

користування тими послугами, які сприймають як ризиковані чи такі, що не викликають довіри [20].

По-третє, фінансові втрати та затримка розвитку інновацій. Кіберзлочинні діяння, такі як фішинг, програми-вимагачі з крадіжкою інтелектуальної власності, завдають прямої шкоди українському бізнесу в Україні. Це, своєю чергою, тягне за собою зростання витрат на ліквідацію наслідків атак та зменшення здатності конкурувати на ринку [71]. І як результат -гальмування приплив інвестицій та призупинення інновації, які є критично важливими для побудови прогресивного інформаційного суспільства.

По-четверте, слід звернути увагу на дезінформацію й операції інформаційно-психологічного впливу (ІПСО). Це стосується залучення соціальних мереж та медійних платформ задля розповсюдження неправдивих відомостей, розпалювання нетерпимості та впливу на погляди загалу. Подібна діяльність негативно позначається на єдності суспільства, спричинюючи його розкол, що, своєю чергою, ускладнює процес ухвалення ключових державних рішень та унеможливлює функціонування єдиного інформаційного поля [2].

Хиткість політичного й фінансового стану, що стримує поступ до розвитку інформаційного суспільства, видається не менш значущим системним викликом на шляху формування та становлення повноцінного інформаційного устрою в Україні. Невизначеність політики та економіки, особливо у світлі тривалого воєнного протистояння, породжує мультиплікативний згубний вплив, який безпосередньо блокує стратегічні інвестиції та надійне розбудовування ІТ-бази та наукового сектору [71].

Політична нестабільність, виражена у зміні основних напрямків, кадрових ротаціях урядовців чи чварах між різними державними інституціями, тягнуть за собою певні результати. Серед них – відсутність сталості у формуванні та впровадженні державних рішень. Суть проблеми полягає у тому, що ключові настанови та плани, скеровані на впровадження цифрових

технологій та розвиток інформаційного простору, нерідко піддаються перегляду або ж безпосередньо припиняють свою дію із приходом нової влади. Це, своєю чергою, унеможливлює доведення до кінця масштабних, фінансово обтяжливих ініціатив (на кшталт розбудови загальнодержавної мережі п'ятого покоління (5G) чи формування уніфікованого корпусу електронних реєстрів). Як наслідок, відбувається розтрата накопиченого досвіду та розпорошення лімітованих фінансових потужностей на задоволення «свіжих» пріоритетів замість неухильного виконання вже затверджених стратегій [79].

Наступне – підрив віри інвесторів. Невпевненість у правилах гри, значні корупційні загрози, а також неминучий ризик для безпеки (зважаючи на війну) – усе це змушує міжнародних інвесторів утримуватися від інвестицій у розбудову інфраструктури зв'язку, телекомунікацій та інноваційних стартапів, що створює серйозні труднощі для країни. У підсумку, держава втрачає надходження життєво необхідних фінансів і передових технологій, які вкрай потрібні для приведення нашої інформаційної сфери у відповідність до глобальних вимог.

Суттєвим завданням, що стоїть перед суспільством, яке базується на інформації, є забезпечення можливості користування інформаційно-комунікаційними засобами. Без стабільного та повсюдного доступу до цих технологій неможливе ані формування, ані подальше просування інформаційного суспільного устрою. Хоча в Україні досить широке охоплення мобільним зв'язком та мережею інтернет, водночас спостерігаються серйозні вади у сфері розвитку інфраструктури та значна нерівномірність у покритті територій, що спричиняє глибинну цифрову нерівність [24].

Бойові дії спричиняють фізичне руйнування необхідної інфраструктури. Масштабне пошкодження телекомунікаційної мережі стало прямим наслідком війни. Базові станції мобільного зв'язку виведено з ладу, а ключові оптоволоконні магістралі та апаратура операторів зазнали пошкоджень на територіях, що перебувають під тимчасовою окупацією чи в зоні

безпосередніх боїв. В результаті, у регіонах, охоплених конфліктом, забезпечення зв'язком часто припиняється зовсім, або ж його відновлення потребує значних інвестицій у фінансах та тривалих часових витрат. Окрім того, це посилює ризики кібератак на життєво важливі системи, адже резервні шляхи передачі даних також можуть бути знищені [45].

З огляду на руйнування та гостру потребу у швидкій відбудові, Україна покладається на зарубіжні технічні розробки, як от супутниковий зв'язок Starlink. Фактично, ми опинилися у стані залежності від закордонної підтримки та технологічних надбань. Незважаючи на те, що подібні системи життєво необхідні для збереження комунікацій під час бойових дій, вони, водночас, породжують технологічну підпорядкованість і потребують суттєвих фінансових вливань для їхнього функціонування та розширення [45].

На тлі розбудови інформаційного суспільства в Україні, що нині переживає особливо інтенсивний військовий період, питання надмірної кількості інформації стає неабияк важливим. Стрімкі та потужні потоки відомостей, які доповнюються спланованими акціями з дезінформування, формують непросте оточення. Це, своєю чергою, безпосередньо відбивається на психологічному стані громадян, а також на їхній спроможності об'єктивно аналізувати отримані дані та зберігати довіру до загальноприйнятих засобів масової комунікації [54].

Перенасичення даними, або інформаційне перевантаження, настає тоді, коли обсяг відомостей, що надходить до індивіда, суттєво перевищує його спроможність цим матеріалом розпорядитися та осягнути його. Це, своєю чергою, відбивається на психіці. Невпинний потік повідомлень (нерідко невтішних, стосовно бойових дій та надзвичайних ситуацій) спричиняє такий феномен, як «втома від інформації», зростання хвилювання, напруги, і, як логічний наслідок, може спричинити «вигорання емоційне» та бажання відсторонитися від будь-яких відомостей взагалі. Внаслідок цього зменшується участь населення у ключових суспільних процесах [11].

Спостерігається занепад здатності мислити критично. Коли мозок людини перевантажений інформацією, він має тенденцію до спрощення процесів і вдавання до використання «коротких шляхів» (евристичних прийомів) з метою оперативного ухвалення рішень. Відтак, люди стають більш вразливими до маніпулятивних технік, привабливих заголовків-«наживок» та емоційно насичених неправдивих відомостей. Як наслідок, загальна здатність громадян розрізняти надійні джерела інформації від сфабрикованих матеріалів та агітації зменшується.

Нездатність населення орієнтуватися у широкому потоці інформації, це спричиняє глибоку кризу довіри. Заразом, усе більше поширюються неправдиві дані та сфабриковані новини. Істотна частка цієї дезінформації, що циркулює в Україні, має чітко сплановану природу й є елементом гібридної війни. Вона активно послуговується можливостями соціальних медіа та анонімних платформ для миттєвого розповсюдження, маючи за мету розколоти суспільство та похитнути віру в державні інституції. Це має прямий наслідок на поширення вигадок щодо державних ініціатив, фінансового стану чи операцій Збройних Сил України, тим самим послаблюючи спроби збудувати стійке та обізнане суспільство [38].

За умов значного соціального напруження медійні платформи та мережі інтернет доволі часто перетворюються на арени для загострення розбіжностей у поглядах, де індивіди схиляються до інформаційних потоків, що лише укріплюють їхні вже сформовані уявлення (явище, відоме як «резонансна камера») [49]. Одночасно із цим, спостерігається спад довіри до класичних, фахових медіа, які, прагнучи дотримуватися принципів валідації даних, піддаються критиці як такі, що є «недостатньо національно свідомими» або, навпаки, «занадто лояльними до влади».

Також маємо справу з питанням розмивання зон відповідальності. У віртуальному середовищі часто доводиться пошукати, аби виявити, звідки ж узялася та чи та інформація. Така ситуація дає змогу різним анонімним

джерелам та програмним роботам без жодних наслідків сіяти сумнівний контент [40]. У результаті, держава й громада змушені залучати багато ресурсів у перевірці фактів та спростуваннях, а не спрямовувати ці інформаційні сили на поступ.

Отже, дослідивши та проаналізувавши виклики на шляху розбудови інформаційного соціуму в України, варто підкреслити: його успішна реалізація прямо пропорційна здатності уряду перетворити оцінені виклики у рушійні сили, що гарантуватиме міцність необхідної бази, захист інформації та розвинені навички аналітичного мислення серед населення [25].

Висновок до розділу 1

Теоретичні основи формування інформаційного суспільства наголошують на його поступовому розвитку. У цьому контексті інформація та набуті знання виступають першочерговими активами, а інформаційно-комунікаційні технології (ІКТ) – вирішальним засобом для перетворення усіх аспектів буття. Розгляд різних концепцій, починаючи від постіндустріальної моделі і аж до суспільства, збудованого на знаннях, виявив його наскрізні ознаки: всесвітню інтеграцію, формування мережевих організацій, пріоритет послугового сектору та збільшення ваги інтелектуального потенціалу особистості.

Ключове значення має державне регулювання у цьому питанні, адже саме воно формує засадничі положення (такі як прозорість та забезпечення рівних можливостей доступу) і визначає інструментарій (зокрема, через законодавчі акти, вкладення коштів у розвиток інфраструктури та освітні програми), які мусять бути задіяні для того, аби технологічний рух сприяв загальному добробуту. У разі відсутності чітко окресленого державного курсу можливе загострення нерівності у сфері цифровізації та некерований, неупорядкований розвиток.

Щодо України, то розбудова інформаційного суспільства обтяжена національними специфіками та зіткненнями з низкою безпрецедентних труднощів: це і гібридні загрози у кіберпросторі та інформаційні наступи, і хисткість фінансового стану, і нагальна потреба у відновленні пошкоджених комунікацій. Для результативного втілення державних ініціатив у цій царині необхідно не лише запроваджувати технічні оновлення, а й забезпечити захищеність від кіберінцидентів, покращити рівень володіння цифровими навичками серед громадян та сформувати зрозуміле правове середовище. Отже, теоретичні основи є тією базою, на якій має бути збудована дієва стратегія, здатна трансформувати наявні перешкоди у стимули для сталої та рівноправної цифровізації українських теренів.

РОЗДІЛ 2

АНАЛІЗ СУЧАСНОГО СТАНУ ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ

2.1. Законодавча та нормативно-правова база державної політики у сфері інформатизації та цифровізації в Україні

Сучасна національна сфера держави знаходиться у фазі динамічного формування, планомірно вливається у всесвітній інформаційний простір та слугує фундаментом для становлення інформаційного суспільства на теренах України.

Побудова інформаційного суспільства в Україні вимагає скоординованих, цілеспрямованих зусиль від усіх державних інституцій та органів муніципального управління, а також послідовного формування та втілення державної стратегії розвитку інформаційного суспільства, що має бути інтегровано як невіддільна частина загальнодержавної політики забезпечення сталого прогресу України [81].

Правове підґрунтя для становлення державної стратегії у царині інформаційного суспільства являє собою збір правових документів, що окреслюють межі, засади та регламенти для всіх суб'єктів, залучених до розробки та впровадження політики у цифровій площині.

Правові засади формування державної політики у сфері інформаційного суспільства – це комплекс нормативно-правових актів, які визначають рамки, принципи та правила для всіх учасників процесу творення та реалізації політики у цифровій сфері [81].

Головним юридичним актом країни є Конституція, де визначені універсальні конституційні засади. Незважаючи на те, що Конституція України не містить прямого посилання на термін «інформаційне суспільство», вона створює базис для його еволюції, закріплюючи [32]:

- Право на інформацію (ст. 34). Унормовує право кожної особи вільно збирати, зберігати, застосовувати та розповсюджувати інформацію, що закладає фундамент для відкритого суспільного простору.

- Право на приватність та захист даних (ст. 32). Життєво необхідно для контролю використання персональних даних у цифрову добу. Фундаментальні засади демократичного урядування та верховенства права, які необхідно трансформувати і в електронний простір.

В Україні ухвалили низку профільних Законів. Цей масив нормативних актів складає ядро правового поля, яке безпосередньо впорядковує взаємодії у секторі, який називають інформаційним суспільством. Зазвичай, вони ухвалюються як відповідь на появу передових технологій та пов'язаних із ними проблем [32].

1. Закони, що регулюють доступ до інформації та електронні послуги

«Про доступ до публічної інформації» (2011) [57]. Цей закон слугує гарантією підзвітності урядових структур, що є фундаментальним елементом «уряду відкритого типу» та зміцнює впевненість громадян у цифрових сервісах.

«Про електронні довірчі послуги» (2017) [58]. Нормативно-правовий акт упорядковує застосування електронних підписів (номінально кваліфікованих), електронних підписів та інших довірчих послуг (формують правову базу для електронного документообігу).

«Про електронні публічні реєстри» (2023) [59]. Це законодавчий акт закладає фундамент для приведення даних до єдиного зразка та забезпечення взаємодії інформаційними потоками поміж урядовими установами.

2. Закони про захист інформації та кібербезпеку:

«Про захист персональних даних» (2010) [62]. Цей нормативний акт фіксує порядок, у якому збираються, опрацьовуються, зберігаються та розповсюджуються персональні дані, що набуває значної ваги у нинішньому середовищі із застосуванням великих даних та ІТ-послуг.

«Про основні засади забезпечення кібербезпеки України» (2017) [67]. Тут окреслюються юридичні та структурні засади охорони життєво необхідних інтересів як особи, так і держави у цифровому просторі, а також встановлюється режим захисту об'єктів критичної інфраструктури.

3. Закони, що стимулюють розвиток IT-індустрії:

«Про стимулювання розвитку цифрової економіки в Україні» (2021) [72] (режим «Дія.City»). Формує особливі регуляторні та фіскальні засади, призначені для підприємств у сфері інформаційних технологій.

4. Закони про цифрову трансформацію:

«Про хмарні послуги» (2024) [75]. Цей акт встановлює правила для розгортання та експлуатації хмарних рішень у державних установах і на об'єктах життєво важливої інфраструктури, метою чого є посилення адаптивності та захищеності інформаційних активів.

«Про національну інфраструктуру геопросторових даних» [64] та низка інших законодавчих актів, спрямованих на регулювання окремих технологічних сфер.

В межах українського правового поля запроваджено низку підзаконних нормативних документів: це як і Укази Президента, так і постанови, що виходять від Уряду, чи накази профільних міністерств. Вони покликані роз’яснювати положення законів та забезпечувати їх практичне втілення.

Наприклад, постанови Кабінету Міністрів, які регулюють роботу Єдиного державного порталу електронних послуг (відомого як «Дія»), встановлюють правила застосування електронних підписів чи визначають норми щодо забезпечення інформаційної безпеки.

Крім того, наявний і певний перелік міжнародно-правових документів. З огляду на те, що інформація не знає кордонів, міжнародні договори набувають вирішального значення.

- Угода про асоціацію з ЄС (пункт про цифрову сферу, узгодження з нормами права Європи) [89].

- Конвенція Ради Європи про кіберзлочинність (мається на увазі Будапештська Конвенція) має на меті приведення у відповідність правових актів держав-підписантів стосовно протидії протиправним діянням у кіберпросторі.

- Директиви та регламенти ЄС (Загальний регламент про захист даних чи Регламент про електронну ідентифікацію та електронні довірчі послуги), які є важливими орієнтирами для України у рамках її прагнення до членства в ЄС.

На початковому етапі організаційної розбудови було засновано Національне агентство України з питань інформатизації, підпорядковане Президентові. Згодом, у процесі реформування державних структур, воно зазнало змін і стало Державним департаментом у складі Міністерства транспорту та зв'язку.

Державні органи, аби втілювати завдання інформатизації, створили структурні підрозділи, які не мали усталеної типової будови чи визначених функцій. Спільна робота державних органів влади координувалася не надто ефективно, через що відомчі інформаційні системи створювалися без прив'язки до загальних потреб взаємодії; формати та стандарти даних залишалися неузгодженими; інформаційні активи держорганів накопичувалися безладно і не бралися до обліку. На тому етапі намічалося запровадження національних норм (стандартів) у сфері інформатизації, розробка загальнодержавних геоінформаційних платформ та пошукових механізмів, формування значних інформаційних ресурсів, налагодження системи захисту даних, а також розвиток вітчизняної сфери програмного забезпечення [22].

Дослідження та інновації цього періоду фокусувалися переважно на технічних аспектах створення інформаційних систем, оминаючи при цьому теоретичні засади опрацювання відомостей, критерії їхньої достовірності, а

також не вирішували питання планомірного та узгодженого впровадження цілей формування інформаційного суспільства [5].

На другому етапі було засновано Державний комітет з питань інформатизації (Держкомінформатизації) як центральний орган виконавчої влади, наділеного функцією спрямування роботи інших центральних органів щодо досягнення цілей збудови інформаційного суспільства та запровадження електронного уряду.

Аналіз стратегічних документів має вирішальне значення для сприйняття напрямку, яким рухається державна політика у царині інформаційного суспільства (далі – ІС) та електронного урядування (далі – ЕУ). Як-от, ці акти (зокрема Концепції, Стратегії, Плани дій) створюють фундамент регуляторної бази, окреслюють вагомі напрямки, бажані вершини, інструментарій впровадження та прогнозовані наслідки цифровізаційних процесів [74].

Державна політика стосовно інформаційного суспільства (ІС) та електронного урядування (ЕУ) в Україні зазнала низки трансформацій, які корелювали зі змінами у технологічному потенціалі та соціальних потреб.

Протягом 2010 року було розроблено Концепцію становлення електронного уряду в Україні, яка слугувала фундаментом для руху до цієї парадигми. Цей документ окреслив головні принципи, а саме порядок взаємин між державними органами та населенням (G2C), так само як і між урядом та бізнес-сектором (G2B). Першочерговими завданнями вважалися створення державних баз даних, забезпечення всього персоналу держструктур доступом до мережі, а також започаткування процесу надання адміністративних сервісів у цифровій формі [74], коли увага змістилася на забезпечення прозорості, протидію корупційним явищам та узгодження національних норм із критеріями Європейського Союзу. Йдеться про Стратегію розвитку інформаційного суспільства в Україні (розраховану до 2020 року) [74]. Цей ключовий документ охоплював як економічні та соціальні сфери, так і

культурні аспекти. Він закладав фундамент для розвитку електронної демократії та електронного урядування, хоча його втілення наштовхнулося на перешкоди через брак коштів та політичну нестабільність. У той період було сформовано концепцію «Держави у смартфоні». Активізувалася імплементація електронних процедур закупівель (система ProZorro) та механізму е-декларування, які згодом стали взірцями успішної цифровізації у сфері протидії корупції.

Сучасна державна політика акцентує увагу на ідеї «Держава у смартфоні» та забезпеченні незламності в умовах бойових дій. Застарілі настанови замінено свіжим, більш далекоглядним планом, який включає концепції цифровізованої економіки та віртуалізованого соціуму – це Концепція та стратегічний напрямок розвитку цифрової економіки та спільноти України [95].

Починаючи з 2022 року, наші стратегічні настанови, зокрема Програми та Плани відбудови, набули суттєвого оборонного та відновного спрямування:

а) особлива увага приділяється децентралізації підходів та активному впровадженню хмарних рішень. Мета цього – гарантувати безперебійне функціонування державних реєстрів, навіть у ситуації повної фізичної втрати відповідної інфраструктури;

б) диджітал-взаємодія з ЄС та НАТО — це пришвидшення узгодження нормативної бази (зокрема, впровадження Загального регламенту про захист даних та законодавчих актів ЄС щодо цифрових ринків), аби укріпити міжнародну співпрацю у питаннях кіберзахисту та безпеки інформації.

в) цифрова допомога громаді – запуск цифрових сервісів для громадян, переміщених у межах країни (ВПО), та стрімке відновлення ключових реєстрів на територіях, звільнених від окупації [76].

У низці стратегічних документів України закладено доволі сміливе та, по суті, слушне бачення руху у напрямку побудови інформаційного суспільства та розбудови електронного урядування. Проте, головний виклик

полягає у спроможності підтримувати сталість та незмінність курсу втілення цих планів, особливо зважаючи на теперішні воєнні реалії, коли критично важлива інфраструктура потребує невідкладного захисту, а громадяни – певних гарантій безпеки та впевненості у надійності цифрової сфери [76].

Підвалини інституційного рівня для формування політики держави в контексті інформаційного суспільства складають органи влади та інші суб'єкти, котрі безпосередньо залучені до процесу створення, ухвалення та впровадження рішень у цифровій царині [76].

Структури, що відповідають за формування та узгодження цієї політики:

1) Загальні напрями державної політики, а також національні плани та стратегічні настанови щодо розвитку інформаційного суспільства (як-от Стратегія розвитку інформаційного суспільства в Україні) схвалюються Кабінетом Міністрів України.

2) Ключовим рушієм інституційного характеру є Міністерство цифрової трансформації України (Мінцифри). Воно несе відповідальність за формування та впровадження державної політики у таких сферах:

- цифровізації, цифрового розвитку, цифрових інновацій та технологій;
- електронного урядування;
- електронних послуг;
- розвитку інформаційного суспільства;
- національних електронних інформаційних ресурсів;
- відкритості даних;
- розвитку IT-індустрії.

Парламентські комітети Верховної Ради України, що спеціалізуються на певних галузях (як от, Комітет, відповідальний за цифрову трансформацію), є центральними органами для формування та опрацювання законодавчих ініціатив.

Щодо національної безпеки та оборони, то Рада національної безпеки і оборони України (РНБО) слугує визначальною координуючою структурою, особливо у питаннях кіберзахисту та стратегічного бачення.

Органи, що забезпечують реалізацію та захист [4]:

1) Технічна та криптографічна безпека інформаційних активів, забезпечення кіберзахисту державних інформаційних ресурсів, а також підтримання працездатності системи захищених комунікацій – це сфера обов'язків Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку).

2) Органи Міністерства внутрішніх справ України, зокрема Національна поліція та відповідні підрозділи кіберполіції, займаються протидією кіберзлочинності та здійсненням досудових розслідувань інцидентів, що трапляються у цифровому просторі.

3) Робота Служби безпеки України (СБУ) спрямована на протидію діяльності розвідок, спрямованій на підривну діяльність у мережі Інтернет, охорону життєво важливих комунікаційних систем та протидію поширенню неправдивої інформації.

4) Міністерство фінансів України відповідає за фінансування ініціатив із цифровізації, що здійснюється коштом державного фінансового резерву.

5) Національний банк України здійснює нагляд за системами платежів, цифровими фінансовими операціями, а також гарантує кібернетичну безпеку у банківській сфері.

6) Органи місцевого самоврядування втілюють заходи цифровізації на рівні областей та міст.

Дорадчі та експертні органи, партнерство.

- Об’єднані громади при державних установах слугують мостом між суспільством та фахівцями.

- Спілки підприємців (включно з ІТ-сектором, Європейська бізнес асоціація) виступають джерелом думок від комерційних структур, сприяючи становленню сприятливих умов для ведення справ.
- Дослідні центри та експертні організації залучаються до творення основних ідей, планів розвитку та оцінки впроваджених рішень.
- Міжнародні партнери: уряди різних держав, глобальні інституції (як-от ООН, Євросоюз, Світовий банк), що надають знання, технічну підтримку та фінансові ресурси.

Взаємодія цих основних принципів має рухливий та повторюваний характер: вони формують вимоги. Приміром, офіційні органи (як-от Міністерство цифрової трансформації чи РНБО) ідентифікують новітні виклики (скажімо, аспекти кібербезпеки) або ж потенційні переваги (нові технологічні досягнення), для яких потрібне запровадження певних правил; після цього створюються юридичні приписи. Так, профільні відомства готують проєкти законодавчих актів чи нижчих за рангом регуляторних документів, неухильно дотримуючись чинного правового поля та міжнародних зобов'язань; законодавчий орган (Верховна Рада) ратифікує закони, Кабінет Міністрів затверджує постанови, надаючи їм юридичної сили; органи виконавчої гілки влади втілюють у життя ухвалені норми, розгортаючи відповідні цифрові послуги, системи захисту та подібне; судова гілка, законодавці, а також громадянське суспільство здійснюють нагляд за тим, наскільки втілення цієї стратегії відповідає встановленим правовим рамкам та її результативність, що може спричинити необхідність змін у правових засадах чи перебудови структури інституцій [4].

Ефективність правочинної системи має вирішальне значення для забезпечення сталості розвитку суспільства, що ґрунтується на інформації, адже саме вона встановлює умови функціонування у цифровій сфері. Здійснити експертизу цієї дієвості означає дослідити як факт існування

потрібного законодавства, так і його спроможність реагувати на постійні зміни, спричинені технологічним прогресом [21].

Маємо низку проблем та показників для визначення рівня дієвості. Стрімкий поступ технологій (таких як ШІ, технологія блокчейн, збір біометричних відомостей) нерідко випереджає діяльність із створення норм. Унаслідок цього нові цифрові взаємодії можуть залишатися поза правовим полем або ж регулюватися актами, що втратили свою актуальність. Дієвість системи оцінюється за метриками швидкості та відповідності адаптації законодавчих актів, включно з тим, наскільки успішно впроваджуються світові настанови (наприклад, Регламент ЄС про захист даних чи Акт про ШІ) [21].

Правова база у сфері інформаційного суспільства мусить гарантувати гармонізацію між численними галузевими законодавчими актами (зокрема тими, що стосуються електронних комунікацій, кібернетичної безпеки та електронного документообігу). Неузгодженість цих норм породжує колізії правового регулювання та ускладнює розбудову дієвого електронного урядування. Ефективність правової системи варто вимірювати через розгляд того, як функціонують уніфіковані електронні реєстри та наскільки вони взаємодіють між собою (інтероперабельність), а також через відсутність розбіжностей між ключовими нормативно-правовими актами (наприклад, між актом регулюючим публічні електронні реєстри та іншими законами відповідних секторів) [21].

Навіть найкращі закони виявляються марними, якщо їх не втілювати у життя. Ця проблема набуває особливої актуальності, коли йдеться про виконання постанов, пов'язаних із збереженням особистої інформації та протидією кіберзлочинності (зокрема, ідентифікацією та покаранням правопорушників). Мірилом успіху слугує ступінь довіри, яку виявляють громадяни та комерційні організації до цифрових послуг та гарантування їхніх законних інтересів. Також береться до уваги діяльність установ, які

здійснюють нагляд (приміром, Державної служби спеціального зв'язку у сфері забезпечення кібербезпеки) [21].

Таким чином, для того, аби держава могла сформувати власну політику у галузі інформаційного суспільства, недостатньо лише того, аби існували відповідні правові засади та інституційна структура; критично важливими є здатність цих елементів до пристосування, еластичність, злагоджена робота та чіткий розподіл функцій. Оскільки технологічний прогрес відбувається надзвичайно динамічно, виникає невпинна потреба у регулярній ревізії та модернізації законодавчих актів, а також у становленні інституцій, які б характеризувалися високим рівнем професіоналізму, результативністю та ефективною координацією між різними відомствами. Тільки за виконання цих передумов держава матиме можливість успішно впоратися з тими нетривіальними викликами, що стоять на шляху до створення інформаційного середовища, яке є одночасно захищеним, прозорим та здатним конкурувати на рівні світової економіки.

2.2. Дослідження ключових напрямків державної політики у сфері інформаційного суспільства

Стрімкий розвиток інформаційно-комунікаційних технологій (ІКТ) докорінно змінив усі аспекти буття, поклавши початок становленню суспільства інформаційного типу. У цьому новому соціумі вирішальну роль відіграють відомості та накопичені знання, які слугують головними активами, а ІКТ є фундаментальним засобом для їх генерації, опрацювання та розповсюдження. Враховуючи цю ситуацію, роль державної стратегії стає наріжною, бо саме вона окреслює контури та умови для продуктивного залучення потужностей ІКТ, зменшення загроз і гарантування розвитку, яке є всеохопним та здатним до самовідтворення [68].

Рис.1



Рис.1. Інформаційно-комунікаційні технології

Становлення суспільства, базованого на інформації, не можна розглядати винятково як технологічний зсув; це також глибоко соціально-економічний та політичний феномен, що потребує застосування цілісного, багатовимірного та міжсекторального підходу. У цій динаміці держава жодним чином не може утримуватися від участі; навпаки, її роль полягає у рішучому формуванні умов, які сприяють інноваційній діяльності, встановленні однакового доступу до цифрових ресурсів для всіх верств населення та забезпеченні надійної захищеності в кіберпросторі [74].

Це дослідження зосереджене на основних курсах державної стратегії, які націлені на формування та вдосконалення інформаційного суспільства. Ми зосереджуємося на тому, якими методами влада підходить до завдання цифровізації економіки та державного адміністрування (електронні послуги), як вона стимулює вдосконалення цифрової грамотності населення, гарантує збереження особистої інформації та підтримує кібербезпеку, а також яким чином вона інтегрує вітчизняне інформаційне середовище у світову цифрову економіку. Знання цих аспектів є вирішальним для якісної оцінки результативності роботи органів влади та встановлення майбутніх пріоритетів розвитку [74].

Наразі інформаційні системи пронизують усі сфери життєдіяльності. Впровадження передових інформаційно-комунікаційних технологій (ІКТ) у комерційній площині спричинило трансформації в електронній комерції, тоді як у державному секторі це дало поштовх до становлення електронного урядування (е-урядування). В Україні процес розбудови е-урядування лише набирає потужності, відправною точкою чого стало започаткування порталу/додатку «Дія». Натомість, у країнах із розвиненою економікою подібна модель взаємодії громадян та суб'єктів господарювання з владними структурами вже є усталеною практикою [74].

В українському контексті, повноваження розпорядчих органів державної влади та органів місцевого самоврядування у сфері інформаційних систем підпорядковані низці законодавчих та підзаконних актів, ухвалених Верховною Радою, Президентом та Кабінетом Міністрів України. Ці правові документи позиціонують застосування актуальних ІКТ та реалізацію політики е-урядування як ключові вектори державної стратегії [95].

Серед ключових показників, що відображають прогрес інформаційного суспільства, виділяється «Індекс розвитку електронного урядування». Цей показник дає уявлення про те, наскільки уряди країн здатні використовувати інформаційно-комунікаційні технології (ІКТ) для надання своїх послуг громадянам. Наразі Україна посідає 69 сходинку у цьому рейтингу серед усіх держав-членів ООН (загальна кількість яких становить 193) [109].

Які кроки були підприємлені Україною для покращення своїх позицій у даному рейтингу протягом останніх двох десятиліть, починаючи з часу проведення Всесвітнього Саміту ООН?

В Україні було запроваджено низку законодавчих актів, зокрема Закон «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [68], а також було затверджено «Стратегію розвитку інформаційного суспільства в Україні» [86], що отримала схвалення відповідною постановою Кабінету Міністрів України. У цій Стратегії,

зокрема, підкреслюється необхідність «формування вітчизняної IT-інфраструктури, надання державної допомоги новосформованим «електронним» галузям економіки, впровадження інформаційно-комунікаційних технологій у всі сфери життєдіяльності (включно з державним управлінням та медіа-сектором), а також удосконалення стану інформаційної безпеки» [74].

Електронне урядування, або Е-урядування, постає як ключовий вектор урядування, метою якого є інтеграція інформаційно-комунікаційних технологій (ІКТ) у функціонування як центральних органів влади, так і органів місцевого самоврядування. Це робиться з метою суттєвого покращення результативності, відкритості та стандарту обслуговування громадян державою, паралельно зі спрощенням та вдосконаленням внутрішніх механізмів управління.

Характеристика основних аспектів розвитку інформаційного суспільства:

Таб.1

Аспекти розвитку ІС	Характеристика
Підходи країн	Різні країни користуються власними підходами щодо побудови ІС, зосереджуючись на різних аспектах ролі та функцій державного сектора та використовуючи різні стратегії.
Державні органи влади	Національні та місцеві органи влади організовують нові установи та структури, що відповідають за формування і розвиток ІС.
Наддержавні органи	Рада Європи та Європейський Союз вивчають механізми розвитку світового ІС.
Основна вимога ЄС	Основною умовою Європейського Союзу з питань ІС є надання громадянам індивідуальних державних послуг, які відповідають їхнім специфічним потребам.
Електронне урядування	Електронне урядування забезпечує надання державних електронних послуг (е-послуг), доступних всім.
Використання Інтернету	Ключовою складовою успішного впровадження електронного урядування є широкомасштабне використання мережі “Інтернет” для надання послуг та їх доступності.
Індивідуалізація послуг	Надання індивідуальних послуг дозволяє кожному обирати форму та спосіб до їх доступу, що робить цей процес більш орієнтованими на потреби громадян.

Таб.1.О. Васильєва, О. Корогодова Формування інформаційного суспільства в Україні в контексті індустрії 3.0: проблеми та перспективи

Е-урядування розвивається з метою реалізації певних важливих завдань:

а) покращення рівня та полегшення доступу до сервісів (переведення надання адміністративних послуг у комфортний електронний вигляд (онлайн цілодобово, без необхідності стояти у чергах, з мінімумом паперової тяганини);

б) зменшення рівня корупційних проявів (обмеження безпосередньої взаємодії між службовцем та особою, яка звертається, уніфікація регламентів та збільшення прозорості у процесі ухвалення ухвал;

в) ощадливе розпорядження коштами (скорочення державних видатків на паперове діловодство та утримання надмірної кількості персоналу);

г) поштовх для економічного зростання (формування сприятливого середовища для бізнесу завдяки оперативного та нескладного процесу отримання необхідних дозволів);

д) залучення спільноти (електронна демократія) (убезпечення апарату для долучення громадян до розробки стратегічних рішень (онлайн-петиції, обговорення, плебісцити).

Таб.2

Компонент	**Назва**	**Суть**
G2C	Government to Citizen	Надання послуг громадянам (наприклад, реєстрація місця проживання, соціальна допомога, отримання паспортів).
G2B	Government to Business	Взаємодія з бізнесом (наприклад, подання податкової звітності, реєстрація підприємств, отримання ліцензій).
G2G	Government to Government	Внутрішня взаємодія між різними органами влади (наприклад, електронний документообіг, обмін даними між реєстрами).

Таб.1. Ключові компоненти е-урядування

Щоб убезпечити вдале впровадження електронного урядування, урядова стратегія повинна зосередити увагу на наступних засадах, що є її визначальними ***напрямами:***

Перший – це формування відповідної цифрової основи та сервісних майданчиків.

Уніфікована платформа електронних сервісів – запровадження єдиного, зведеного пункту, через який можна отримати доступ до будь-яких державних послуг (як-от мобільний застосунок та вебсайт «Дія» в Україні).

Е-урядування є однією з центральних ланок у процесі цифровізації України. Надання громадянам можливості скористатися державними послугами через цифрові інтерфейси для комунікації з владними структурами, що втілено, наприклад, у порталі «Дія», дає змогу суттєво оптимізувати витрати часу населення на вирішення різноманітних питань у режимі реального часу, включаючи реєстраційні процедури для бізнесу чи оформлення довідок. Як наслідок, це суттєво полегшує як процес надання, так і процес отримання цих послуг, паралельно підвищуючи загальну продуктивність органів виконавчої влади [36].

Слід наголосити, що зростання рівня володіння цифровими навичками як серед населення, так і серед держслужбовців, виступає вирішальним елементом для успішної реалізації електронних сервісів. Адже за умови неспроможності користувачів повноцінно ними скористатися, будь-які зусилля із їхнього розгортання стають беззмістовними. Йдеться не просто про переведення застарілих процесів у цифровий формат, а про докорінну перебудову системи взаємодії між державою, суспільством та комерційними структурами, яка базується на концепції «Держава-Платформа» та принципі «орієнтація на людину» [69].

Електронні системи комунікації. Запровадження захищеного каналу передачі відомостей між державними реєстрами (система «Трембіта»), що унеможливлює необхідність громадян надавати повторно ті самі папери (принципи «цифрове за замовчуванням» та «одноразове подання») [76].

Хмарні технології. Міграція державних інформаційних систем у стійкі та інтегровані хмарні середовища задля оптимізації фінансового навантаження та підвищення рівня безпеки.

Другий напрям - цифрові ідентифікаційні й електронні довірі послуги.

Кваліфікований (КЕП) чи удосконалений (УЕП) електронний підпис: необхідно сприяти всебічному запровадженню кваліфікованого електронного підпису як ексклюзивного юридично визнаного засобу для здійснення електронної комунікації.

Ідентифікація через мобільний застосунок: запровадження надійних, але водночас спрощених методів підтвердження особистості дистанційно, використовуючи мобільні мережі чи банківські сервіси, задля отримання доступу до різних послуг [76].

Третій – це перетворення адміністративних послуг: зміна підходу з моделі, що працює «на вимогу клієнта», на модель, де держава ініціює та надає послугу у моменти настання певної життєвої обставини (на кшталт появи дитини або зміни реєстрації місця проживання). Йдеться про впровадження комплексних сервісів, прив'язаних до життєвих подій, та повний перехід державного сектору на електронний документообіг, що означає відмову від паперового обміну документами між установами [76].

Четвертий – гарантування кібернетичної безпеки й охорони інформації – полягає у формуванні міцного захисту проти кібернападів на життєво важливі інформаційні системи та у захисті особистих даних: імплементуються європейські норми щодо оперування даними (на кшталт засад, подібних до Регламенту про загальний захист даних), а також підтримується таємність і дається змогу мешканцям контролювати відомості про себе [20].

Отже, розвиток у сфері електронного урядування — це не просто оновлення, а стратегічна інвестиція у майбутнє держави. Те, наскільки вправно втіляться ці кроки, окреслить, наскільки країна є цифровою, настільки швидко вона зможе давати раду складнощам і як добре впишеться у

загальносвітовий цифровий простір. Це є життєво необхідне для того, щоб піднести конкурентну перевагу та зміцнити суспільну довіру до державних органів.

Хоча є чималі здобутки, з-поміж яких особливо виділяється електронне урядування (Е-урядування) та надання послуг у цифровій формі (це одне з найбільш відчутних досягнень, скажімо, запуск мобільної програми «Дія»), щоб політика й надалі була дієвою, необхідно опанувати низку суттєвих, вирішальних завдань.

У нинішньому суспільстві, де панує інформація, а державні реєстри, грошові потоки, енергетична інфраструктура та зв'язок цілковито покладаються на цифрові технології, питання інформаційної безпеки та кіберзахисту перетворилося з простої технічної потреби на наріжний камінь безпеки держави.

Інформаційна безпека, по суті, є таким станом захищеності життєво важливого інформаційного простору, за якого гарантується недоторканність, вірогідність та оперативність доступу до даних. Йдеться про багатогранну стратегію, яка інтегрує у себе правові норми, управлінські заходи, етичні принципи та технологічні рішення [39].

Кібербезпека (або ж кіберзахист) є невід'ємною частиною загальної інформаційної безпеки. Вона фокусується на забезпеченні захисту цифрового середовища – а саме мереж, апаратних і програмних комплексів, а також інформації, що ними обробляється, – від будь-яких неправомірних втручань. Йдеться про запобігання несанкціонованому доступу, використанню, розголошенню, пошкодженню, зміні чи повному знищенню даних, спричиненому кіберагресією, шпигунством у мережі, тероризмом у кіберпросторі чи іншими ворожими акціями.

Існує три основні принципи інформаційної безпеки [39]:

1) конфіденційність, яка полягає у недопущенні ознайомлення з даними сторонніх осіб, забезпечуючи доступ лише тим, хто має на те повноваження (захист особистих відомостей);

2) цілісність, що означає підтвердження достовірності, повноти відомостей та відсутності будь-яких змін, внесених без належного дозволу;

3) доступність (гарантування того, що уповноважені особи можуть отримати доступ до даних та систем безперебійно та у необхідний час).

Основні напрями державної політики у зазначеній галузі мусять мати системний характер та охоплювати численні аспекти, включаючи правові, інституційні та технічні складові.

Одним із найважливіших аспектів сьогодення постає забезпечення безпеки життєво важливих інформаційних систем (ЖВІС). Даний напрямок має чітко окреслені критерії та поділ на класифікації цих активів (сфери енергетики, фінансові структури, транспортні мережі, засоби комунікації), збій у роботі яких здатний спричинити серйозні наслідки для оборонної спроможності країни, економічного стану чи повсякденного буття громадян [64].

З огляду на поточні життєві реалії, надзвичайно актуальними постають вимоги у площині кібербезпеки, зокрема запровадження уніфікованих та обов'язкових засадничих норм і стандартів (як-от ті, що базуються на ДСТУ чи ISO) для всіх суб'єктів, які володіють чи управляють критичною інформаційною інфраструктурою (КІІ), стосовно гарантування її захисту.

На державному рівні запроваджується нагляд, метою якого є формування та підтримка роботи загальнодержавної системи для розпізнавання кібератак на об'єкти критичної інформаційної інфраструктури (КІІ) та протидії цим загрозам. Подальший розвиток інституцій та формування правової бази відбувається через стратегічне планування: Національна стратегія кібербезпеки регулярно переглядається, аби відповідати сучасним реаліям загроз. Національна система реагування на кіберінциденти (CERT-

UA), разом із галузевими та відомчими центрами, отримує необхідну підтримку та сприяння у своєму розвитку. Правова основа, що регулює захист відомостей, обмін даними, а також визначення відповідальності за діяння у сфері кіберзлочинності та кібертероризму, формується через ухвалення відповідних законодавчих та підзаконних актів [73].

Ще одним важливим аспектом виступає нарощування потенціалу у сфері кібербезпеки та підготовка відповідних кадрів. Заплановано та реалізовано відповідним чином урядом спеціалізовані формування військового та правоохоронного спрямування (що відображено у загальнонаціональних планах) з метою ефективного стримування ворожих дій у віртуальному просторі та ефективної протидії шпигунській та деструктивній активності.

Актуально, просвітництво та наукова діяльність складають наразі невід'ємні елементи державній політиці України. На сьогодні здійснюється кардинальна перебудова системи фахової підготовки й удосконалення навичок кадрів у царині кіберзахисту та цифрових технологій; заохочуються наукові й інженерні проєкти у сфері протидії кіберзагрозам; зростає рівень обізнаності широкого загалу та державних чиновників із питань медіа-компетентності й обізнаності у кіберпросторі [73].

Спостерігається жваве розгортання співпраці та входження у міжнародні структури. Наявність України у міжнародних структурах та системах для обміну даними про кібернетичні небезпеки та найкращими практиками є фактом. Вітчизняні підходи, методики та інструменти для гарантування кіберзахисту гармонізуються з визнаними стандартами ЄС та НАТО. Бо ж у контексті цифрового століття кібербезпека стає життєво необхідною умовою для збереження державності, що передбачає недопущення зовнішнього втручання у внутрішні процеси, охорону державних інформаційних активів та забезпечення життєдіяльності економіки. Це стосується безперебійної роботи фінансових, енергетичних та

телекомунікаційних галузей. Водночас посилюється довіра населення до механізмів захисту особистих даних та безпечного користування електронними сервісами [73].

Насамперед, захист життєво важливих інформаційних систем та державних реєстрів даних мусить залишатися у фокусі уваги. З огляду на тривалу зовнішню агресію та безперервні кіберзагрози, стратегічний курс держави спрямований на посилення резистентності ключових об'єктів гармонізацію правил кібербезпеки з усталеними стандартами НАТО та Європейського Союзу, а також нарощування внутрішнього потенціалу щодо ідентифікації та нейтралізації кіберподій. Насамперед, захист життєво важливих інформаційних систем та державних баз даних мусить залишатися у фокусі уваги. З огляду на тривалу зовнішню агресію та безперервні кіберзагрози, стратегічний курс держави має бути спрямований на посилення резистентності ключових об'єктів життєво важливих інформаційних систем, гармонізацію правил кібербезпеки з усталеними стандартами НАТО та Європейського Союзу, а також нарощування внутрішнього потенціалу щодо ідентифікації та нейтралізації кіберподій [73].

Отже, вкладення коштів у кібербезпеку – це, по суті, інвестиції у міцність, сталостість та самостійність суспільства, що базується на інформаційних технологіях.

У нинішньому інформаційному світі цифрова обізнаність набула такого ж базового значення, як і е-управління та пропонування електронних сервісів, гарантування інформаційної цілісності та захисту у кіберпросторі. Її сутність полягає у спроможності індивіда безпечно, з користю та усвідомлено оперувати інформаційно-комунікаційними засобами (ІКТ) у кожній сфері буття: професійній діяльності, здобутті знань, відпочинку та взаємодії [48].

Прогрес у сфері опанування цифрових компетенцій виступає принциповим напрямом державної програми, адже саме це гарантує включеність суспільства у інформаційний простір, не допускаючи при цьому

розриву у доступу до цифрових технологій. Коли ж населення не має потрібного рівня володіння цими навичками, воно неспроможне ефективно застосовувати можливості електронного урядування, електронної торгівлі чи ресурсів для навчання в мережі, що, своєю чергою, гальмує сукупний суспільно-економічний підйом.

В Україні вже функціонує чимало мережевих ресурсів, починаючи з платформ для перегляду контенту та закінчуючи урядовими веб-ресурсами.

Загалом, мережею користується більше, ніж дві третини громадян нашої країни. Однак, досі залишається частина – близько третини українців – які не мають змоги підключитися до всесвітньої павутини. Найбільше ця проблема зачіпає мешканців сільських районів, де спостерігається незадовільний рівень сигналу, а прокладання кабельного зв'язку може обійтися надто затратно [48].

Запорукою сучасної розбудови стало те, що це питання нині виходить на перший план для нашої держави, а урядові структури та оператори телекомунікацій мають намір довести мобільний інтернет до кожного куточка країни. З цією метою держава виділила частоти у смузі 800–900 МГц для впровадження технології 4G, що дозволило забезпечити зв'язком понад двісті тисяч громадян України лише за період із липня до листопада 2020 року. Проте, подальший поступ у цьому напрямку був призупинений з 2022 року і має поновитися не раніше 2026 року; наразі ж покриття мобільним доступом забезпечено на основних міжнародних та важливих внутрішніх транспортних артеріях [48].

З огляду на це, протягом наступних трьох років уряд має намір сприяти здобуттю цифрових умінь для більш ніж 6 мільйонів наших співвітчизників.

Отже, в Україні в найближчі роки значна частина населення не просто отримає можливість користуватися мережею, а й повноцінно задіє всі її потенціали. Криза, спричинена пандемією, чітко продемонструвала життєву потребу у якісному підключенні та втрати, що виникають через його

відсутність. Тому активне розгортання технології 5G буде лише на руку та посприяє скороченню уявного цифрового розшарування [48].

Щороку спостерігається зростання числа громадян, які мають змогу користуватися мережею Інтернет. До того ж, покриття 4G-технологіями охоплює вже 80% населення планети, і очікується, що до 2026 року ця частка сягне 95%. Бачимо явну тенденцію до покращення ситуації від року до року, однак підтримка заходів, спрямованих на зменшення розриву у доступі до цифрових технологій, залишається критично важливою. В Україні повноцінне функціонування 5G поки що відсутнє, хоча вже здійснюються пробні активації. На теперішній час мережі п'ятого покоління працюють в експериментальному режимі у вибраних місцях, а повномасштабне розгортання цієї технології очікується не раніше 2030 року, з огляду на пріоритети у сфері оборони. Водночас, із розширенням зони покриття 5G, очікується зростання потреби у сучасних онлайн-сервісах. Йдеться про телемедицину та дистанційне навчання, інтегроване з технологіями доповненої/віртуальної реальності, де критично важливими є як наднизька затримка сигналу, так і бездоганна стабільність з’єднаннят [74].

Подальше впровадження передових технологічних рішень принесе суспільству низку нових перспектив. З огляду на це, необхідно вже зараз зосередитися на розвитку цифрових компетенцій населення, аби задовольнити майбутні вимоги ринку праці, що, своєю чергою, стимулюватиме зростання як валового внутрішнього продукту держави, так і економіки в цілому [94].

У сфері цифрових навичок найважливішими є такі аспекти: обізнаність у царині інформації та даних (вміння шукати, критично оцінювати та організовувати відомості й дані); взаємодія та спільна робота (ефективне застосування цифрових інструментів для спілкування та групової діяльності); генерування цифрового контенту (уміння створювати, редагувати й комбінувати різні формати цифрових матеріалів, як-от тексти та медіа); захищеність та цифрова гігієна (забезпечення безпеки обладнання, інформації,

приватної життєдіяльності та добробуту); розв'язання питань (виявлення необхідності у цифрових рішеннях та усунення технічних проблем).

Державна політика повинна охоплювати всі вікові та соціальні верстви населення, формуючи єдину національну освітню екосистему. Як приклад, це передбачає розробку єдиних національних стандартів та навчальних планів. Країна мусить запровадити загальнонаціональні стандарти цифрових компетенцій (наприклад, базуючись на європейській моделі DigComp), які б окреслювали мінімально необхідний рівень цифрових умінь для кожного мешканця, а також інтегрувати цифрову грамотність як суворий обов'язковий елемент на усіх освітніх щаблях – від ясел до університетів; необхідно запровадити регулярне підвищення кваліфікації для викладацького складу, аби гарантувати їхню спроможність якісно і сучасно передавати цифрові знання; слід заснувати локальні та регіональні осередки цифрового навчання (скажімо, при бібліотеках чи центрах надання адміністративних послуг), а також ініціювати спеціальні проєкти для літніх людей, котрі становлять найбільш уразливу категорію щодо ризику цифрової ізоляції; необхідно гарантувати можливість користування навчальними матеріалами та ІКТ-інфраструктурою в сільських районах та невеликих населених пунктах; окрім того, важливо створити навчальні посібники та інтерфейси, адаптовані під потреби осіб з обмеженими можливостями здоров'я [94].

На сьогодення розробляються великі освітні ініціативи та співпраці, метою яких є запуск загальнонаціональних, відкритих для всіх, безоплатних навчальних майданчиків із підтвердженою інформацією задля масового опанування громадянами цифрових умінь (приміром, загальнодержавні вебсайти, присвячені цифровій освіченості).

Співпраця між державою та приватним сектором також набирає обертів. До створення навчальних планів та надання навчальних матеріалів долучають комерційні організації (фірми у сфері ІТ, фінансові установи, оператори мобільного зв'язку) як елемент їхньої соціальної місії. Яскравим прикладом

такої взаємодії слугує налагоджена співпраця щодо вдосконалення цифрових знань учасників навчального процесу між Державним університетом інформаційно-комунікаційних технологій, з одного боку, та Sense Bankом, АТ «ПриватБанк», компанією Huawei та іншими, з іншого.

З погляду на те, як оцінюється та відстежується національне дослідження у цьому аспекті, слід підкреслити, що систематично здійснюється опитування громадської думки та тестування з метою досягнення неупередженого вимірювання рівня володіння цифровими навичками серед населення та ідентифікації прогалин недопрацювання. Паралельно з цим, запроваджується механізм добровільної атестації цифрових компетенцій, що, своєю чергою, збільшує їхню вагомість у контексті попиту на ринку праці.

Державні інституції спрямовують ресурси на розвиток цифрової освіченості, що продукує комплексний позитивний наслідок: зростає здатність робочої сили конкурувати на ринку праці та стимулюється перехід до економіки, орієнтованої на цифрові технології. У сфері державного адміністрування спостерігається активне впровадження електронних сервісів (е-урядування), що веде до підвищення продуктивності державного сектору. Що стосується системи соціального забезпечення, то відбувається зміцнення спроможності громадян протистояти інформаційним маніпуляціям, неправдивим повідомленням та мережевому шахрайству, що є невід'ємною складовою забезпечення інформаційної безпеки [94].

Тому, після аналізу головних орієнтирів державної стратегії у сфері формування інформаційного простору України, можна констатувати її багатогранність та комплексний характер, скерований на досягнення країною належного рівня цифровізації через узгодження дій у трьох взаємозалежних площинах: технічне забезпечення, державні органи та людські ресурси.

Для того, аби держава могла успішно втілювати політику, спрямовану на розбудову інформаційного суспільства, абсолютно необхідною є скоординована робота різних відомств, а також налагоджений, безперервний

обмін думками із комерційними структурами та громадськістю. Окрім того, ключовою умовою є забезпечення стабільного фінансування для розвитку як технічної бази, так і програм навчання. Саме цей всеохоплюючий метод дасть змогу нашій країні повноцінно розкрити свій потенціал у сфері технологій, гарантувати власну обороноздатність і гармонійно приєднатися до європейського цифрового середовища [80].

2.3. Аналіз проблем та бар'єрів у реалізації державної політики у сфері інформаційного суспільства в Україні

Попри відчутний поступ та сміливі заміри у сфері діджиталізації, втілення державно-політичних рішень щодо розбудови інформаційного суспільства в Україні наштовхується на низку усталених перепон та труднощів. Ці чинники гальмують швидкість імплементації новітніх рішень, несуть загрози для сталості безпекових аспектів та посилюють розрив у соціальній сфері.

Одним із найвагоміших структурних обмежень, що стоять на заваді ефективному виконанню державної стратегії в галузі інформаційного розвитку та цифрового перетворення України, виступає неузгодженість правової бази. Це породжує обставини правової невизначеності, стримує інвестиції капіталовкладень і робить складнішим процес впровадження передових технологічних здобутків [48].

Основоположним негативним моментом є неупорядкованість та застарілість нормативно-правового поля. Регулювання діяльності у сфері інформаційних технологій відбувається через низку різнорідних правових документів, що походять із різних галузей права (наприклад, цивільного, адміністративного, торговельного чи кримінального). Унаслідок цього спостерігається брак цілісного, організованого бачення, що значно ускладнює процес імплементації норм права на практиці [48].

У сфері законодавства простежується певний технічний розрив, оскільки чинні нормативно-правові акти нерідко не встигають за швидким темпом технологічного прогресу. Це найвиразніше помітно у регулюванні передових галузей, як-от штучний інтелект (ШІ), де бракує чітко визначених механізмів розподілу відповідальності за рішення, ухвалені ШІ-системами, а також у сфері оперування масивами даних, що зумовлює невизначеність щодо правового статусу цих даних як економічних ресурсів, створює труднощі у встановленні належної юрисдикції та порядку збереження життєво важливої державної інформації, а також стосовно криптовалют і технології блокчейн: незважаючи на кроки до їх легалізації, зберігається нагальна потреба у комплексному врегулюванні питань їхнього обігу та оподаткування [48].

Маємо колізії між регуляторними актами, що походять з різних рівнів (як-от закони та похідні нормативні документи), а також між актами, що належать до різних сфер права (наприклад, коли норми щодо кіберзахисту перетинаються з тими, що стосуються обробки особистих даних). Це породжує юридичні труднощі, з якими стикаються як комерційні структури, так і державні установи.

Попри те, що впровадження електронного документообігу вже доволі значне, все ще простежуються перешкоди на шляху повної цифрової трансформації, що вказує на недоробки у функціонуванні електронного документообігу. Хоча законодавство і надає електронним документам повної юридичної ваги, на рівні реального впровадження виникають складнощі з можливістю взаємодії електронних систем документообігу між різними установами влади, і частина державних структур досі не готова остаточно відмовитися від паперових носіїв [91].

Також існує проблема запровадження світових норм. Вона полягає у повільному чи неповному втіленні основних європейських розпоряджень та постанов (скажімо, GPДР у питанні захисту особистої інформації та правових

актів ЄС стосовно безпеки в кіберпросторі), що ускладнює зближення українського діджитал-середовища з європейським.

Складнощі виникають у сфері управління, а саме – відсутності дієвих юридичних інструментів для формування регуляторних «майданчиків» – особливих правових умов, які дають змогу підприємствам, що впроваджують новинки, випробувати свої розробки та сервіси без загрози порушення чинних законів, що стримує прогрес ФінТеху й інших інноваційних галузей [48].

Ще однією відчутною перепоною у впровадженні державних рішень стосовно інформаційного суспільства є відсутність чіткого законодавчого поля у сфері кібербезпеки. Це породжує утруднення у визначенні переліку об'єктів критичної інфраструктури. Процедура виявлення та категоризації об’єктів критичної інформаційної інфраструктури є надмірно забюрократизованою та не відповідає реальному рівню загроз, що, своєю чергою, негативно позначається на дієвості їхнього захисту.

Суттєвою сучасною проблемою, особливо в умовах військових дій з боку російської федерації проти України, є труднощі з проведенням кіберрозслідувань. Прогалини у нормативно-правовій базі ускладнюють здійснення швидких та результативних розслідувань у кіберсфері (особливо коли задіяні іноземні юрисдикції) та притягнення до відповідальності осіб, винних у вчиненні кіберзлочинів [1].

Недостатність правових норм, що регулюють обмін відомостями про кібернетичні загрози, свідчить про відсутність налагодженої процедури для швидкого та безпечного обміну даними про інциденти у сфері кібербезпеки між державними установами та приватними організаціями, що, своєю чергою, породжує вразливі місця у масштабах усієї держави.

Вирішення цих питань потребує багаторівневої стратегії: необхідно здійснити перевірку (аудит) чинних актів законодавства, ухвалити основоположні закони стосовно цифровізації (цифрової трансформації), а також запровадити системи регулярного відстеження та гнучкого

припасування правової бази до тих інновацій, що з'являються у технологічній сфері.

Нестача персоналу – то одна з найнагальніших проблем, що стримує здатність державних інституцій дієво втілювати політику в галузі інформаційного соціуму. Спостерігається гостра нестача фахівців високого ґатунку у сфері ІТ, проєктувальників систем, фахівців у питанні кіберзахисту та аналітиків даних у владних структурах як на центральному, так і на регіональному рівнях [1].

Ситуацію загострюють такі чинники:

1) недостатня конкурентоспроможність винагороди: рівень оплати праці у публічному секторі суттєво поступається тому, що пропонує приватна ІТ-індустрія (зокрема, коли мова йде про світовий ринок праці). Це призводить до того, що урядові структури неспроможні ані привабити провідних експертів із ринку, ані втримати ефективно тих, кого вже підготували;
2) інтенсивний відтік кадрів. Навіть ті молоді та здібні професіонали, яким вдалося потрапити на державну службу, нерідко її покидають. Причинами є слабка стимуляція, в'язкість адміністративних процедур та обмежені перспективи для стрімкого кар'єрного розвитку;
3) бракує керівних фахівців: відчувається не лише нестача тих, хто виконує технічні завдання, але й очільників цифрових ініціатив та керівників, відповідальних за цифрову перебудову (CDTO), котрі володіють потрібним баченням, кваліфікацією в керуванні складними ІТ-ініціативами та вмінням узгоджувати дії між різними структурами [1].

Водночас, спостерігається послаблення інституційної стійкості та захищеності, що виражається у дефіциті кваліфікованих працівників. Це прямим чином позначається на сталості та безпековому рівні державних

механізмів. Дана ситуація, своєю чергою, породжує загрози у сфері кібернетичної безпеки. Дефіцит експертів із кіберзахисту та цифрової гігієни у структурах влади зумовлює те, що державні інформаційні ресурси залишаються піддатливими до зловмисних втручань. Це може варіюватися від нерозуміння конфігурування засобів захисту до помилок, спричинених людським чинником [1].

Складнощі виникають у процесі як підтримки, так і подальшого зростання цього сегменту. Зважаючи на дефіцит вітчизняних фахівців, зокрема розробників та системних архітекторів, уряд нерідко опиняється у становищі повної залежності від компаній-підрядників з-за кордону, навіть коли мова йде про забезпечення життєво необхідних програмних комплексів. Такий стан речей значно збільшує потенційні загрози, стосовно поширення ноу-хау та втрати управлінських важелів, а також ускладнює будь-які спроби швидкого внесення змін чи вдосконалення цих систем [71].

На жаль, є не менш суттєва проблема у втіленні державної політики стосовно інформаційного суспільства – це коли органи влади впадають у «технологічний ступор». Установам, яким бракує фахівців з технічних питань, властиво ухилятися від запровадження новітніх, хоч і складніших, проте значно дієвіших технологій (скажімо, застосунку Штучного Інтелекту чи хмарних сервісів), побоюючись, що не зможуть належно їх обслуговувати та використовувати [27].

У межах українського цифрового простору, як і будь-якого іншого, простежуються недосконалості у внутрішніх механізмах – так званий бюрократичний спротив. Запровадження новітніх цифрових засобів регулярно наштовхується на протидію з боку працівників, які або не володіють достатніми цифровими навичками, або не вбачають для себе персональної користі від автоматизації процесів. Це, своєю чергою, спричиняє ігнорування нововведень чи їх некоректне застосування [27].

Спостерігається невисока якість управління проєктами, а також відсутність спільної цифрової парадигми. Через недостатній рівень обізнаності в застосуванні гнучких методологій та управління масштабними цифровими ініціативами, реалізація запланованих кроків затягується, кошториси перевищуються, і часто кінцевий результат не збігається з первинно поставленими завданнями.

У багатьох урядових установ досі не сформована внутрішня цифрова культура, яка б передбачала відкритість, оперативне ухвалення рішень, що ґрунтуються на інформації (з використанням даних), та сприйнятливість до безперервних трансформацій.

Вирішення проблеми слабкості інституційної бази потребує всеосяжної реорганізації системи державної служби: включаючи коригування рівня винагороди, впровадження гнучких механізмів залучення ІТ-спеціалістів (наприклад, шляхом співпраці держави та приватного сектору), а також широкомасштабне вдосконалення компетенцій наявних кадрів [1].

Попри чималі старання, матеріально-технічне підґрунтя та стан захищеності віртуального середовища в Україні все ще лишаються чинниками системних негараздів, що заважають формуванню всеосяжного суспільства знань.

Як уже слушно зауважено, наявна є проблема «цифрової нерівності».

Поняття «цифровий розрив» вказує на дисбаланс у спроможності різних прошарків суспільства та територій користуватися інформаційно-комунікаційними технологіями, що знаходить вияв у нерівномірності забезпечення широкосмуговим зв'язком. Тоді як у містах рівень покриття (включаючи мобільні мережі 4G/5G) є досить високим, то у сільській, гірській та важкодоступній місцевості якісний, високошвидкісний та, що найбільш важливо, фінансово прийнятний інтернет-доступ або суттєво обмежений, або взагалі відсутній [48].

Такий стан речей безпосередньо унеможливлює повне включення громадян до користування електронними сервісами (е-урядування), оскільки люди не спроможні отримати доступ до переваг цифровізації. Ба більше, це гальмує поступ у сферах навчання на відстані, телемедичних послуг та електронного комерційного обігу у відповідних регіонах, тим самим посилюючи економічну та соціальну нерівність

Нерідко бракує життєво важливої первинної інфраструктури, як-от оптоволоконних ліній, веж телекомунікаційного зв'язку та апаратури для підключення кінцевих споживачів. Це зумовлює потребу у великих грошових вливаннях, на які приватні провайдери зважуються не завжди охоче, особливо коли точаться бойові дії, якщо немає державної допомоги [27].

Це породжує низку суттєвих загроз: ускладнюються процеси злиття систем, зростає ймовірність аварій та зупинок у роботі (унаслідок недостатньої стійкості до відмов), а також виникає значна вразливість для кібернетичних нападів через те, що патчі безпеки не підтримуються в актуальному стані.

Не маючи узгодженої хмарної політики, міграція державних реєстрів та інформаційних комплексів на передові, захищені хмарні середовища гальмується, ускладнюється централізований контроль, знижується раціональність поводження з даними та призводить до зростання фінансових витрат на експлуатацію [48].

Наразі спостерігається наявність значних труднощів у сфері кібербезпеки та забезпечення стійкості. Забезпечення захисту в цифровому середовищі постає як завдання найвищого пріоритету, де державне регулювання стикається з унікальними перешкодами. Ми бачимо перманентний характер цілеспрямованих атак у кіберпросторі. Українська держава потерпає від безпрецедентного обсягу та високого рівня кібератак (особливо тими, що націлені на об’єкти критичної інформаційної інфраструктури, фінансові установи та державні структури). Це зумовлює необхідність безперервного залучення матеріальних засобів та підтримки

постійно високого стану боєготовності, що створює неабиякий тягар як у фінансовому, так і в кадровому плані [71].

За міжнародними розрахунками, Україна посідає одне з чільних місць у світі за обсягом, потужністю та заплутаністю цілеспрямованих кібератак. Сей тип втручань має стратегічну мету та нерідко зав'язаний на військових і дезінформаційних кампаніях.

Складнощі виникають у процесі виявлення та забезпечення безпеки об'єктів критичної інфраструктури (КІІ): процедура визначення та категоризації таких об'єктів відбувається повільно, а реальний стан їхнього захисту та перевірка здатності протистояти кіберзагрозам не завжди відповідають прийнятим світовим нормам. Це, своєю чергою, несе небезпеку для обороноздатності держави, адже збій функціонування цих об'єктів може спричинити руйнівні наслідки. За міжнародними розрахунками, Україна посідає одне з чільних місць у світі за обсягом, потужністю та незрозумілістю цілеспрямованих кібератак [71].

Складнощі виникають у процесі виявлення та забезпечення безпеки об'єктів критичної інфраструктури (КІІ): процедура визначення та категоризації таких об'єктів тягнеться повільно, а реальний стан їхнього захисту та перевірка здатності протистояти кіберзагрозам не завжди відповідають прийнятим світовим нормам. Це, своєю чергою, несе небезпеку для обороноздатності держави, адже збій функціонування цих об'єктів може спричинити руйнівні наслідки.

Протистояння невпинним складним загрозам тягне за собою потребу у значних фінансових, логістичних та людських активах, аби осучаснити оборонні механізми, придбати найновіші захисні системи, забезпечувати функціонування національних підрозділів реагування (CERT-UA) та гарантувати безперебійну роботу систем цілодобово [48].

Слабка культура кібербезпеки (людський аспект) є не менш суттєвою перешкодою. Попри наявність найсучасніших засобів захисту, людина

залишається найбільш вразливою частиною системи. Нехтування елементарними нормами безпеки та недостатня обізнаність державних службовців щодо загроз фішингу та прийомів соціальної інженерії відкривають прості можливості для несанкціонованого проникнення до державних систем [48].

Наразі спостерігається недостатньо організована, швидка та надійна система взаємодії та обміну інформацією про нові кібернебезпеки та події між урядовими структурами (зокрема СБУ, Держспецзв'язку, CERT-UA) та приватними суб'єктами критичної інформаційної інфраструктури (КІІ). Це, своєю чергою, уповільнює загальну спроможність до спільного реагування [27].

Отже, для досягнення стійкості інформаційного суспільства необхідні не лише інвестиції у технологічні аспекти, а й суттєві інституційні зміни у сфері кіберобезпеки, а також культивування й піднесення рівня цифрової грамотності на усіх етапах.

У сфері розбудови інформаційного суспільства фінансові та економічні чинники, як-от обмеження, є серйозною перешкодою для державної політики. Йдеться про забезпечення фінансування, яке є нестійким та цілком залежить від зовнішніх донорів. Багато значних цифрових ініціатив (зокрема процес запровадження новітніх платформ та уніфікованих стандартів) надто покладаються на міжнародну технічну підтримку та грошову допомогу від спонсорів. Це, своєю чергою, породжує загрози нерегулярності фінансових надходжень та зміщує національні пріоритети. Створення та втілення у життя ґрунтовних, надійних та взаємосумісних (інтероперабельних) інформаційних технологічних рішень потребує суттєвих інвестицій, які часто неможливо гарантувати коштом державного бюджету [71].

Ускладнений доступ до державних закупівель стає перешкодою на шляху до впровадження інновацій. Процедури державних закупівель, як правило, є складними та займають багато часу, що відлякує інноваційний

бізнес від долучення до державних проєктів. Обмежена державна підтримка наукових досліджень та розробок у царині ІКТ стримує формування національних інноваційних продуктів, змушуючи державу покладатися на інпортні технології.

Здійснення державної стратегії щодо формування інформаційного суспільства обумовлюється не лише наявністю технологій та коштів, але й готовністю та здатністю населення – як державних службовців, так і громадян – сприймати та опановувати цифрові трансформації. Саме тут виявляються суттєві перешкоди, пов'язані із соціумом та людським фактором [27].

Крім того, спостерігається протидія змінам та інертність, притаманна державному апарату. Значний організаційний та психологічний спротив впровадженню новітніх цифрових засобів та процедур походить від певної когорти державних службовців.

Фактори, що зумовлюють цей опір:

- острах перед передовими технологіями та ризиком втрати працевлаштування внаслідок автоматизації процесів;
- відсутність наполегливості та небажання опановувати нові робочі методики;
- нездатність усвідомити користь від цифрових інструментів, що спричиняє формальне, поверхове впровадження цифровізації (друк документів, отриманих в електронному вигляді);
- відсутність «цифрового мислення» [27].

Певний відсоток населення та бізнесу досі виказує недовіру до офіційних державних програмних комплексів, через побоювання щодо захищеності особистої інформації або беручи до уваги минулий невдалий досвід. Це чинить перешкоди для цілковитого переходу на електронне ведення документації й відмову від паперових носіїв.

Низька комунікація спричиняє ситуацію, коли державні органи не завжди спроможні забезпечити зрозумілу комунікацію щодо вигоди та

надійності нововведених цифрових сервісів. Нерідко основний акцент робиться саме на аспекті технічної реалізації, а не на тій користі, яку це приносить безпосередньо споживачеві, і це гальмує масове впровадження [27].

Подолання цих соціальних аспектів потребує не лише навчальних програм, а й цілісного плану управління трансформаціями в органах влади, що був би націлений на стимулювання, здобуття знань та утвердження цифрової культури

Ці бар'єри свідчать, що успішна зміна цифрового ландшафту вимагає не лише впровадження технологій, а й суттєвого реформування на рівні інституцій, персоналу та фінансового забезпечення.

Висновок до розділу 2

Проведений аналіз сучасного стану та втілення державної стратегії у царині інформаційного суспільства та цифровізації на території України, свідчить про наявність амбітної програми перетворень та помітних зрушень у впровадженні основних цифрових проєктів.

Базисна правова основа для цифровізаційних змін була вибудувана, особливо стосовно електронного врядування та забезпечення кібернетичного захисту. Однак, вона досі має суттєву розпорошеність та не встигає за швидкістю технологічного прогресу, що спричиняє виникнення юридичних неузгодженостей та уповільнює процес врегулювання використання передових технологій (ШІ, Big Data) [27].

Державна політика зосереджує свої зусилля на чотирьох ключових напрямах: просуванню електронного урядування (з акцентом на успіхи у сфері надання цифрових сервісів), гарантуванні кібербезпеки (через невпинну боротьбу з кібернетичними викликами), підвищенні рівня цифрової грамотності населення та заохоченні зростання цифрової економіки.

У процесі втілення державної політики у сферу інформаційного суспільства постає низка фундаментальних перепон: 1) спроможність

інституцій залишається замалою; 2) відчутна нестача кваліфікованих ІТ-фахівців у державному апараті спричинена неконкурентоспроможністю грошової винагороди; 3) продовжує існувати розрив у сфері цифрового доступу, зокрема щодо широкосмугового інтернету у сільських районах, а також застаріле технологічне забезпечення у державних структурах; 4) серйозні загрози кібербезпеці вимагають постійних та суттєвих інвестицій для забезпечення захисту критичної інформаційної інфраструктури, тоді як захист особистих даних залишається загрозливим через людські помилки та неузгоджені державні реєстри; 5) спостерігається небажання сприймати нововведення та низький рівень цифрової обізнаності серед певної категорії держслужбовців і громадян, що гальмує широке застосування електронних сервісів.

Таким чином, Україна засвідчила рішучість у напрямі цифровізації. Проте, аби вийти за межі лише впровадження окремих послуг і збудувати повноцінне, стійке та доступне для всіх інформаційне середовище, необхідна не просто модернізація технічних засобів, а фундаментальна перебудова інституційної спроможності, кадрового потенціалу та нормативно-правової бази. Майбутні досягнення тепер залежатимуть від спроможності уряду гарантувати стабільне фінансування, заповнити критичні вакансії та зміцнити кібербезпеку на всіх рівнях функціонування.

РОЗДІЛ 3

ШЛЯХИ УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ

3.1. Стратегічні пріоритети та напрямки оптимізації державної політики у сфері інформаційного суспільства з урахуванням європейського досвіду

Інтенсивний розвиток у сфері інформаційно-комунікаційних технологій (ІКТ) на тлі світових тенденцій цифровізації кардинально змінює усі аспекти існування, висуваючи перед державою як нові труднощі, так і небачені раніше перспективи. Формування суспільства, зосередженого на інформації та базованого на знаннях, — то не просто тренд, а життєво важлива стратегічна умова для збереження конкурентоспроможності, забезпечення стабільного економічного розвитку та покращення добробуту населення. Реалізація цього напряму потребує всеохоплюючої, узгодженої та гнучкої державної стратегії, яка б спромоглася встигати за стрімкими трансформаціями та вміло інтегрувати набуті успіхи європейських країн у цій галузі [21].

Аби збудувати те, що зветься «суспільством знань», життєво необхідною є стратегія розвитку інформаційного простору народу. Йдеться про такий устрій, де для розвитку як окремої особистості, так і економіки та держави в цілому, найважливіше — здобувати, зберігати, творити та поширювати відомості, зважаючи при цьому на ключові інтереси України.

Основне завдання, яке ставить перед собою національна стратегія розвитку інформаційного суспільства, полягає у покращенні рівня буття українців, забезпеченні конкурентоспроможності нашої держави на світовій арені, стимулюванні зростання у сферах господарства, соціуму, політики, культури та духовності, а також у вдосконаленні механізмів державного управління через упровадження сучасних інформаційних технологій [21].

На нашу думку, формування інформаційного суспільства є стратегічною метою соціально-політичного маркетингу, яка має ґрунтуватися насамперед на національних пріоритетах і спрямована на формування сприятливого образу нашої держави як суб'єкта світової геополітики. «Соціально-політичний маркетинг використовує інструменти брендингу не лише всередині країни, а й має на меті створити бажаний імідж країни на міжнародній арені. Брендинг країни може включати різний набір факторів та атрибутів, але він також тісно пов’язаний зі специфічними рисами соціально-політичної системи» [9].

Для України, як і для кожної іншої держави, що прагне відігравати значущу роль на міжнародній арені, характерна наявність чітко визначених національних пріоритетів. Насамперед, це стосується розвитку людського капіталу – суспільства, орієнтованого на людину, де належна увага приділяється пошані людської гідності, а також дотриманню прав та свобод кожного громадянина. Другим ключовим аспектом є гарантування інформаційної стійкості як для населення, так і для самої держави, що є особливо актуальним з огляду на поточні військові дії. По-третє, Україна має на меті посилення власної значущості у світовому гуманітарному та культурному вимірах, активно просуваючи власну культуру. Перевірений досвід передових країн свідчить про високу результативність застосування концепції «м’якої сили», розробленої Джозефом Наєм, у процесі такої популяризації. Четвертим напрямком є вдосконалення механізмів державного управління, стимулювання економічного зростання та розвитку соціального сектору. І, нарешті, п’ятим імперативом є побудова сучасної цифрової економіки [21]. «Стратегія розвитку інформаційного суспільства» закріплює за кожною особою право на вільний доступ до відомостей та можливість самостійно обирати способи здобуття знань під час опрацювання даних. Під час акумулювання, фіксації та розповсюдження відомостей, що стосуються як фізичних осіб, так і установ, обов'язковим є дотримання чинного

законодавства. Це, своєю чергою, означає, що будь-яке несанкціоноване вилучення чи поширення персональних даних карається згідно із законом. Отже, на державу покладається обов'язок забезпечення захисту прав та інтересів громадян України у сфері інформації [21]. Проте, на практиці ця ситуація не завжди відповідає задекларованому.

Слід також зауважити, що відсутні міжнародно-правові інструменти, які б гарантували суверенітет нашої країни, навіть у межах національних частин Інтернету. Це ставить під сумнів їхній «цифровий суверенітет». «Сьогодні відповідальність держави передбачає принцип поваги до цифрового суверенітету. Адже сучасне поняття суверенітету державу означає не лише суверенітет кордонів, але стосується також і кіберпростору… Всі країни є рівноправними учасниками кіберпростору, всі мають рівні права на доступ до нього» [74]. Хоча багатостороння (за участю багатьох зацікавлених сторін) модель керування Інтернетом має право на існування, державам, які беруть участь у цій моделі, необхідно мати змогу забезпечувати захист своїх громадян.

Кожна держава у світовій павутині має свої власні інтереси. Покладатися на те, що ці інтереси будуть задоволені завдяки зусиллям транснаціональних ІТ-гігантів, замість використання власних національних ресурсів, є нереалістичним. Це питання безпосередньо стосується національної безпеки, оскільки засилля міжнародних інтернет-корпорацій спричинить монополізацію ринків, межі яких не визначені державним суверенітетом [74].

З огляду на забезпечення цифрового захисту та незалежності, суверенні держави мусять усвідомлювати, що контроль над глобальною інфраструктурою наразі утримується могутніми «гігантами корпоративного світу» й перебуває поза юрисдикцією міжнародного правового поля. Проте, ситуація докорінно змінюється. Дедалі більше громадян усвідомлюють, що світова мережа більше не слугує тим високим ідеалам, для яких вона була

започаткована. Зрештою, пріоритетом має бути гуманітарний розвиток людства. Як слушно підкреслює нинішній науковець Фан Біньсін: «Інтернет повинен бути інструментом для вільного доступу до інформації та її поширення, а не місцем, де корпорації полюють за особистими даними мільярдів користувачів» [10].

Аби утвердити власний суверенітет, українським підприємствам у сфері інтернету конче необхідно втримати провідні позиції на вітчизняному ринку та гарантувати фундаментальний рівень інфраструктурного забезпечення: від телекомунікаційних послуг і програмного забезпечення до розробки та функціонування інформаційних систем.

У перспективі - це необхідність поступового переходу на вітчизняні рішення для криптографічного захисту інформації, а також на українське апаратне, програмне забезпечення та власну компонентну базу. Крім того, це торкається розробки загальнодержавного та прикладного програмного забезпечення, телекомунікаційного устаткування та апаратних засобів, призначених для активного вжитку серед населення, суб'єктів господарювання, державних інституцій та органів місцевого самоврядування [70].

Отже, першочерговим осередком уваги у цій «Стратегії» є забезпечення незламності інформаційно-телекомунікаційної інфраструктури держави, а саме – унеможливлення таких дій, як підміна, викривлення, блокування, вилучення, від’єднання від каналів зв’язку та всіляких інших маніпуляцій із даними. Крім того, планується запровадження єдиної, централізованої системи для нагляду та керування усією мережею електрозв’язку України, а також гарантування здатності українського сегменту Інтернету функціонувати безперебійно, надійно та автономно

Ключова складова проблеми тотальної інформатизації полягає у концентрації контролю над порядком переміщення даних у мережі в межах однієї сфери впливу. Країни, як і колись, фактично виступають у ролі «малих

інвесторів». Однак, на даний момент, міжнародна структура, відома як «Форум з управління Інтернетом» (Internet Governance Forum), заснована під егідою ООН у 2006 році, пропонує інший підхід – «багатосторонню модель управління» Всесвітньою павутиною. Основне завдання цього Форуму – усунення розриву в цифровому розвитку між державами. Урядам, які зараз мають статус «міноритаріїв» у чинній системі, доцільно консолідувати зусилля та спільно відстоювати правові інтереси своїх громадян.

Ключовою складовою загальнонаціональної стратегії формування суспільства, заснованого на інформаційних технологіях, виступає гарантування фундаментальних прав та свобод громадян, серед яких - право на особисте життя, недоторканність конфіденційних даних і подібне. Приміром, на цей час кожен, хто проживає у межах Європейського Союзу, володіє законним правом висунути вимогу до пошукової системи Google щодо деактивації посилань на веб-ресурси, що містять персонально-ідентифіковану інформацію [21].

У травні 2018 року Європейський Союз запровадив у дію Загальний регламент щодо захисту даних (General Data Protection Regulation, GDPR). Цей нормативний акт наділяє кожного, хто проживає в ЄС, повноваженням вимагати, щоб жодна установа чи суб'єкт, який опрацьовує дані, не надавав доступ до вебсторінок, що містять особисті відомості про користувачів, котрі вважаються «застарілими й не мають суспільної важливості» [70].

Водночас в Європейському Союзі точаться дебати щодо того, наскільки індивід може розпоряджатися відомостями про себе, що вже опубліковані у вільному доступі. Крістіан Мір, очільник німецького представництва «Репортери без кордонів», наголошує: «У подібних ситуаціях критично важливо знайти баланс між тим, що цікаво громадськості, та правом особи на недоторканність її приватних даних» [38].

На думку експерта, коли мова заходить про свободу слова та доступу до відомостей, інтернет-прайм на забуття являє собою, по суті, «хибне

нововведення». Це пов'язано з тим, що визначення межі між правом вільно отримувати дані та необхідністю охоронити персональну інформацію наразі зосереджене у руках комерційних структур. Крістіан Мір зазначає: «Звернення громадян із вимогою видалити посилання на ту чи іншу інформацію про них розглядає не суд, а спеціально створена в кожній окремій державі комісія експертів при концерні Google» [38]. Він також підкреслює, що «право на забуття» в мережі має потенціал для неправомірного використання, оскільки «ним можуть скористатися, наприклад, особи, які уособлюють тоталітарні режими, для того, щоб інформація, яка їм не до вподоби, зникла з Інтернету» [там само].

Фахівці схиляються до думки, що стосовно кримінальних діянь, скоєних раніше, зокрема серйозних, як-от убивство, доцільно продовжувати зберігати відповідну інформацію у мережі Інтернет протягом значного проміжку часу. При цьому остаточне вето на тривале утримання цих даних або їхнє усунення мало б належати судовій інстанції, яка б керувалася аргументацією від експертних груп організацій-власників пошукових сервісів та уповноважених осіб державних структур. Проте у ситуаціях менш суттєвого характеру законодавчі норми виглядають виправданими [78].

У час загального цифрового поглинання, громадянам необхідний хоч якийсь ступінь захисту особистого життя, де «право на приватість» часом стає надзвичайно слушним інструментом. На думку правників-експертів, питання про те, чи варто видаляти певні відомості з інтернету, має вирішуватися лише у прив’язці до кожного окремого випадку. Фундаментом сучасних прав людини у віртуальному просторі є одночасно право на доступ до відомостей та право на недоторканність приватних даних. З огляду на це, ключовим об'єктом для роздумів філософів, політологів та юристів має залишатися пошук рівноваги між волею слова та особистою таємницею [68].

Стосовно України, у нас досі відсутнє законодавче регулювання права на анонімність у мережі, або «права на приватність». З нашої перспективи,

враховуючи курс на євроінтеграцію та розбудову цифрового суспільства, нагальною є потреба у приведенні українського законодавства у відповідність до норм Європейського Союзу. Актуальність ухвалення закону про право на приватність полягає передусім у наданні громадянам механізму примусу інтернет-платформ до видалення даних про особу, які втратили свою актуальність або є недостовірними [68].

У ракурсі оборони державних інтересів та з огляду на викладене вище, головні ідеї стосовно впровадження стратегії інформаційного суспільства можуть бути такими:

• збереження культури й української самобутності;

• забезпечення кібербезпеки громадян нашої держави, зокрема дітей та молоді;

• створення надійного інформаційного простору через розповсюдження відомостей про джерела, котрі сприяють поширенню традицій українських духовних й етичних цінностей;

• удосконалення й упровадження навчальних методик, зокрема тих, що передбачають віддалене навчання, а також активне впровадження електронних освітніх платформ;

• забезпечення можливостей для поширення надбань української культури та наукових досягнень у міжнародному просторі; розбудова світового визнання української мови;

• виховання у громадян високих моральних засад і глибокого розуміння правових норм, а також формування культури споживання медіа та відповідального застосування інформаційно-комунікаційних засобів;

• формування та просування комплексних систем, що надають нормативну, правову, консультативну, технологічну та технічну підтримку у сфері ідентифікації, нейтралізації, унеможливлення та протидії загрозам інформаційній безпеці населення;

• оптимізація процесу обмеження доступу до інформації, обіг якої заборонено законодавством, і забезпечення її вилучення;

• модернізація регуляторних інструментів, що стосуються діяльності засобів масової інформації, інтернет-мовлення, соціальних платформ, веб-ресурсів та засобів обміну повідомленнями;

• впровадження кроків для раціонального використання актуальних інформаційних просторів з метою розповсюдження правдивої та високоякісної інформації вітчизняного походження;

• забезпечення насичення ринку фінансово доступними, добротними та санкціонованими медіа-контентами і сервісами, виготовленими в Україні [44].

Державна програма розвитку інформаційного суспільства ґрунтується на визначених на довготривалий час орієнтирах у соціально-економічній, науково-технічній та національно-культурній сферах розвитку держави. При цьому враховуються глобальні вектори та здобутки у сфері грамотної інформатизації, що є ключовим елементом для забезпечення інтеграції України у світовий інформаційний простір [68].

Слід підкреслити, що формування світового інформаційного середовища, яке реагує на актуальні тренди інформаційної геополітики, становить значущий елемент державної стратегії стосовно розвитку інформаційної інфраструктури на теренах України.

Державна програма щодо розвитку технічного забезпечення інформаційної сфери являє собою комплекс взаємозалежних даних, мета яких – втілення у життя політики держави та головних шляхів формування актуальної ІТ-бази України. Це відбувається через ефективне використання фінансових, матеріальних та технічних резервів, виділених на певні трансформаційні місії (проєкти), а також шляхом узгодження інших джерел, виробничих та науково-технічних потенціалів країни, діяльності державних органів, структур місцевого самоврядування, комерційних та некомерційних організацій, незалежно від форми власності, та громадян у галузі

інформаційних технологій. Ініціативи та заходи, націлені на формування, розширення та об'єднання інформаційних мереж, систем, активів і технологічних рішень, котрі передбачають закупівлю обладнання для роботи з інформацією (чи його складників) з метою вдосконалення роботи установ загальнодержавного значення, місцевих виконавчих органів, інших установ та організацій, фінансуються з бюджетних асигнувань і виконуються у межах загальнодержавної програми інформатизації [68].

Стратегія державного управління у питанні регулювання та відтворення інформаційного соціуму має на меті піднесення національної конкурентоспроможності, переважно через розвиток здібностей людей у галузях з високим рівнем інтелекту. Вона слугує запорукою економічного поступу та покращення добробуту через надання зручного доступу до інформації та широкого використання інформаційно-комунікаційних технологій. Державна політика спрямована на формування нових робочих місць та розширення перспектив зайнятості населення, збудування передової та захищеної цифрової бази, а також забезпечення безпечної роботи ключових систем життєзабезпечення держави. Це підтримує формування прозорих, демократичних спільнот, які гарантують дотримання основоположних прав громадян щодо їхнього залучення до суспільних процесів та участі у формуванні рішень на рівні як державної, так і територіальної влади [46].

3.2. Розроблення комплексу заходів щодо удосконалення державної політики у сфері інформаційного суспільства

На часі перед Україною постає нагальне завдання концептуально осмислити запровадження інформаційного вектора у життєустрій суспільства. Фактично, це означає, що будь-які плани щодо розбудови фундаменту інформаційного суспільства мусять бути інтегровані у ширший спектр стратегічних цілей держави, що стосуються соціального поступу, економічного зростання та інституційних реформ. Такий підхід позиціонує

інформатизацію як ключовий, невід’ємний елемент глибинної трансформації як самого суспільства, так і державних структур.

Як відомо, для розвитку інформаційного суспільства необхідна комплексна методологія. Ця методологія мусить охоплювати стратегічне бачення процесу інформатизації, визначення конкретних пріоритетів, а також гармонізацію з поточними соціально-економічними, політичними та культурно-історичними реаліями, де світовий досвід відіграє ключову роль. Крім того, такий підхід нерозривно пов'язаний із загальною динамікою економіки та держави [4]. Успішна реалізація цього методу можлива виключно за умови збалансованої взаємодії трьох основних секторів – держави, приватного бізнесу та громадськості, – які повинні мати реалістичні завдання та достатню політичну рішучість.

Перш за все, потрібно виробити та впровадити цілісну державну стратегію формування інформаційного суспільства, яка б відповідала сьогоденним реаліям. Ця стратегія повинна охоплювати впровадження заходів, спрямованих на прогрес інформаційного суспільства у політичному, правовому, економічному, соціокультурному та технологічному вимірах.

Спираючись на цю розроблену стратегію розвитку інформаційного суспільства, слід підготувати детальний план кроків та визначити конкретні дії для її виконання, інтегруючи при цьому настанови від українських громадських формувань, бізнесу, науковців та міжнародних інституцій.

Варто підкреслити, що правова база, котра регулює сферу інформаційної інфраструктури, має бути доопрацьована та покращена, особливо у таких аспектах:

- створення концепції інформаційного законодавства нашої держави, що визначатиме процедури створення та впровадження відповідних регуляторних документів, а також їхню структуру та інтерпретацію;

- підготовка проектів законів, спрямованих на регулювання процесів створення, застосування, збереження та поширення інформаційних активів країни;

- кроки з метою стимулювання та розвитку національної індустрії програмного забезпечення.

- опрацювання відомостей у цифровій формі, а також, у першу чергу, керування документообігом, надання їм офіційного статусу;

- посилення державної системи захисту інформації, охорони національних інформаційних ресурсів та приватної інформації;

- формування уніфікованого стандарту для ІТ-рішень,

- гармонізація вітчизняного законодавства з міжнародними актами стосовно атестації інформаційних засобів тощо.

Подолання цих проблем дасть змогу розкрити більше можливостей українського сектору інформаційних технологій та сприятиме глибшому входженню нашої держави у світову спільноту, що оперує інформацією.

З огляду на викладене, оновлення правової бази у сфері інформації має відбуватися поступово: спершу – ухвалення оновленого варіанту ключового Закону України «Про інформацію» [63] та внесення поправок до суміжних законодавчих актів; і лише після цього – упорядкування усього інформаційного законодавства через процес кодифікації. А саме – створення Інформаційного кодексу України, який би консолідував усі складові цього правового напряму [5].

Завдання вдосконалення державної стратегії у сфері інформаційного суспільства в Україні має охоплювати низку різнобічних проєктів, націлених на оновлення та модернізацію вітчизняної інфраструктури інформаційних мереж і систем. До таких кроків, зокрема, можна віднести розширення доступу до широкосмугового Інтернету та інших цифрових сервісів, зміцнення кіберзахисту, а також стимулювання впровадження передових технологічних рішень та розвитку підприємництва у цьому секторі. Окрім того, державний

курс може акцентувати увагу на збільшенні кількості кваліфікованих ІТ-кадрів та інтенсифікації застосування інформаційних технологій у навчальних закладах і надання державних послуг [70].

Державна політика стосовно інформаційної інфраструктури має бути спрямована на стимулювання випуску інформаційних продуктів, послуг зв'язку та оперування даними, водночас посилюючи встановлену потребу в них. Фактичне впровадження національних установок у цій царині в умовах сучасної України демонструє розгорнуту психологічну акцію, її суспільне кредо та докази дієвості у формуванні схвального сприйняття її основних елементів серед населення. Для успішного виконання цієї стратегії потрібен комплекс кроків, що прийнято називати інформатизацією [76].

Політична сфера у галузі інформаційного суспільства набула динаміки лише відносно нещодавно, коли дійшло усвідомлення потреби у формуванні в Україні осередку знань — як ключової передумови для політичної та суспільно-економічної прогресії, а також стало зрозуміло, наскільки важливо берегти позитивний імідж держави та її статус на міжнародній арені.

На нашу думку, низка кроків, котрі є обов'язковими для вдосконалення державної стратегії в аспекті інформаційного суспільства, включає наступне:

1) Покращувати дієвість та рівень надання послуг в електронному форматі.

Швидкісна цифрова трансформація утвердилася як одна з вирішальних течій XXI століття, що докорінно змінює усталені засади взаємодій між урядовими структурами, населенням та комерційними підприємствами. У світлі цих подій, електронне врядування (е-врядування) постає не лише як набір технічних засобів, а як центральний важіль для оновлення системи державного керування, гарантуючи її відкритість, високу продуктивність та відповідальність перед суспільством.

В умовах глобальної конкуренції та невизначеності у сфері міжнародних відносин, особливо зважаючи на розв'язану повномасштабну

війну, здатність держави протистояти кіберзагрозам стає першочерговою. Міцність же цієї стійкості значною мірою залежить від дієвості електронного врядування та високої якості послуг, що надаються у цифровий спосіб. Це дає змогу гарантувати безперебійне функціонування державного апарату навіть під час надзвичайних обставин; раціоналізувати роботу державних структур, знижуючи тягар зайвої паперової тяганини та пришвидшуючи процес ухвалення життєво важливих рішень; а також зміцнити довіру населення до державних органів через забезпечення відкритості та легкого доступу до необхідних відомостей [48].

Здійснивши відчутний крок уперед у процесах цифровізації, що значною мірою підкріплено втіленням новаторських підходів, Українська держава мусить безперервно оновлювати та вдосконалювати стратегії стосовно електронного врядування. Мета – не просто наздоганяти, а мати перевагу над тими викликами, що постають із технічного прогресу.

Аби підняти на вищий щабель дієвість електронного урядування та покращити якість надання електронних послуг, потрібен багатогранний план дій, який би зачіпав як інституційні трансформації та оновлення технічної бази, так і нарощування потенціалу людських ресурсів та узгодження з нормами Європи [76].

Стосовно настановок, слід акцентувати увагу на таких моментах:

- впровадження європейських зразків співпраці між державними інституціями, зокрема у питанні транскордонного обміну інформацією;

- віднесення якості надання електронних сервісів до рівня, який відповідає європейським критеріям, особливо у контексті захисту особистих даних (згідно з GDPR) та забезпечення кібернетичної безпеки;

- досягненні повного доступу (інклюзії) до цифрових сервісів для усього суспільства, що розглядається як наріжний камінь європейського соціального курсу;

- покращення результативності електронного врядування та добротності електронних сервісів приносить відчутний економічний та суспільний зиск;

- убезпеченні від зловживань: зменшення можливостей для корупції через обмеження особистої взаємодії службовця з громадянином під час обслуговування;

- оптимізації видатків із державної скарбниці, пов'язаних із паперовим документообігом та утриманням застарілих адміністративних процесів;

- формуванні належних умов для здійснення підприємницької діяльності завдяки оперативним та зрозумілим електронним етапам отримання дозволів та реєстрації;

- гарантуванні громадянам спрощеного та миттєвого отримання доступу до соціального, медичного та освітнього забезпечення [76].

Отже, напрацювання добре аргументованих пропозицій щодо покращення результативності електронного урядування та покращення якості послуг в електронному форматі є нагальною потребою для досягнення сталого прогресу України, посилення її інтеграції до європейського простору та зведення до реальності цифрової спільноти, що фокусується на запитах людей.

2) Вдосконалення сфер безпеки в цифровому просторі [94].

Ключовим кроком на шляху розвитку цифрового загалу в Україні мусить бути зміцнення захисту в мережі. Покращення досяжне за умов впровадження більш жорстких регламентів та надання ясніших настанов. Для побудови стійкого цифрового середовища потрібен багатогранний підхід до забезпечення кіберзахисту, а саме:

1. Покращення нормативно-правової бази в аспекті кіберзахисту з огляду на вимоги ЄС та НАТО, а також посилення ключових елементів Національної системи кібербезпеки (зокрема, Держспецзв’язку, СБУ та Кіберполіції)
2. Повна гармонізація вітчизняного законодавства та практик обробки персональних даних відповідно з Європейським генеральним

регламентом про захист даних (GDPR). Довіра виступає засадничим активом епохи цифровізації. Забезпечення належного рівня приватності та неухильний нагляд за опрацюванням даних не лише зміцнюють віру населення в електронні сервіси, а й становлять обов'язкову передумову для інтеграції України до європейського простору обміну інформацією [76].

3. Оновлення технічного оснащення та захист критичної інфраструктури: впроваджувати передові розробки для нагляду, ідентифікації та протидії кіберподіям (наприклад, центри оперативного реагування – SOC, системи керування подіями безпеки – SIEM), а також регулярно здійснювати перевірки захищеності та спроби зламу. Необхідно підвищити здатність системи кіберзахисту шляхом формування та вдосконалення Оперативних центрів реагування на кібернетичні інциденти (SOC) для усіх ключових інформаційних систем та державних установ. Зважаючи на те, що кібератаки стають частішими та складними, ефективний контроль та оперативні дії є єдиним шляхом гарантувати безперебійну роботу електронних сервісів та збереження державної інформації.
4. Організувати загальнонаціональні акції, спрямовані на покращення обізнаності населення з питань кібербезпеки, а також імплементувати курси з інформаційної безпеки у навчальні плани на всіх рівнях освіти, що критично важливо для формування необхідних фахових кадрів.
5. Міжнародна взаємодія: посилення співпраці із закордонними союзниками (такими як Сполучені Штати, Європейський Союз, НАТО, а також спільнотами CERT) задля двостороннього обміну даними розвідки щодо загроз та залучення технічної підтримки [2].

Кібербезпека є не виключно технічним питанням, а, радше, наріжним каменем для належного становлення інформаційного устрою в межах України. Якщо ми не зможемо забезпечити надійність та суспільну довіру до

віртуального середовища, то увесь хист інформаційно-комунікаційних технологій для стимулювання економіки та зміцнення демократичних інституцій залишиться невикористаним, а громада опиниться під загрозою з боку деструктивних чинників, як зовнішнього, так і внутрішнього походження [71].

3) Просувати цифрові навички.

Аби вдосконалити державну політику у сфері інформаційного суспільства, необхідно планомірно піднімати рівень цифрових знань державних службовців. Це означає запуск обов'язкових та періодичних курсів для опанування цифрових умінь, кіберзахисту та застосування найсучасніших ІКТ для усіх держслужбовців. Якість електронного урядування прямо залежить від того, наскільки підготовлені й спроможні чиновники працювати в цифровій екосистемі. Без належної кваліфікації можуть виникнути серйозні проблеми з наданням послуг громадянам.

Також потрібно заохочувати зростання цифрової обізнаності серед населення. Слід продовжувати втілювати державні ініціативи, спрямовані на підвищення рівня цифрової грамотності громадян, акцентуючи увагу на старшому поколінні та мешканцях сіл, залучаючи для цього різноманітні форми навчання (вебінари, центри надання адміністративних послуг, бібліотеки). Якщо громадяни не володіють цифровими навичками, це стає головним бар'єром для загального користування електронними сервісами. Вкладення у підвищення обізнаності – це, по суті, інвестиції у майбутній попит на цифровізацію.

4) Збільшувати інвестиції.

Аби покращити державну політику стосовно інформаційної інфраструктури України, ключовим кроком має стати нарощення вкладень в інтернет-інфраструктуру, особливо в сільській місцевості. Для цього доречно залучати як пряме державне фінансування, так і механізми державно-приватного співробітництва. Окрім того, не обійтися без створення

загальнонаціонального плану розвитку широкосмугового доступу, який би окреслив чіткий вектор поширення послуг швидкісного інтернету по всій території країни. Цей план зобов'язаний ідентифікувати території з найменшим покриттям і чітко розставити акценти, куди саме спрямовувати інвестиційні зусилля першочергово [76].

5) Впроваджувати принципи та дії інституційної бази.

Слід законодавчо впорядкувати та запровадити технічні засоби для реалізації принципу «єдиного контакту», сутність якого полягає в тому, що особі (громадянину чи суб'єкту господарювання) необхідно подавати будь-який документ чи відомості до державного органу лише одноразово. Відтепер державні служби мусять здійснювати обмін потрібними даними між собою через захищені комунікаційні шляхи. Такий підхід суттєво послабить тягар бюрократії, прискорить розгляд звернень, покращить ступінь задоволеності громадян та бізнесу, а також мінімізує можливості для корупції. Цей принцип є фундаментальним, що встановлений у загальноєвропейських Інтероперабельних настановах [22].

Окрім того, необхідно запровадити посаду «Власник даних», яка б чітко окреслювала сферу відповідальності та повноваження певних державних інституцій (міністерств, апаратури) як первинних розпорядників державних реєстрів та інформації, що в них зберігається. Цей механізм гарантуватиме достовірність, своєчасність та належний рівень даних у точці їхнього первинного накопичення, що є життєво важливим для безперебійного функціонування усіх електронних сервісів, які спираються на цю інформацію.

Здійснити ґрунтовну перебудову всіх управлінських процесів, акцентуючи увагу на послідовності «життєвих подій» (поява новонародженого, переїзд, започаткування підприємницької діяльності), а не на внутрішній ієрархії чи відділах державних установ. Такий підхід уможливить розробку інтегрованих (згрупованих) електронних сервісів, які зводитимуть до купи операції різних служб в межах однієї цифрової форми,

тим самим забезпечуючи максимальну простоту та логічну ясність для користувача [48].

6) Заохочувати до проваджень нових технологій.

Належним чином діятимуть заходи, спрямовані на стимулювання запровадження передових технологій, зокрема 5G і Інтернету Речей (IoT), адже вони слугуватимуть наріжними каменем для формування інформаційного суспільства в межах України. Реалізація цього можлива через запровадження субвенцій та податкових преференцій для підприємств, які вкладатимуть кошти у вдосконалення цих саме технологічних рішень.

Питання забезпечення сталої сумісності (міжоперабельності) набуває найвищої ваги – варто докласти зусиль для досягнення високого ступеня інтеграції між усіма державними інформаційними ресурсами та реєстрами, використовуючи єдиний захищений майданчик (система «Трембіта», що є фундаментальним складником цифрової інфраструктури країни) та стандартизуючи протоколи передачі відомостей (API).

Необхідно приділити значну увагу аспектам користувацького досвіду та інтерфейсу (UX/UI). Слід запровадити обов'язкові вимоги до оформлення (дизайну UX/UI) та забезпечення доступності (інклюзивності) для усіх електронних сервісів та державних веб-ресурсів. Регулярно організовувати перевірку зручності використання із залученням справжніх користувачів. Оцінка якості електронних послуг споживачем відбувається не лише з огляду на швидкість роботи, а й на те, наскільки вони комфортні, зрозумілі та скільки натискань мишкою вимагають. Відмінний рівень UX/UI безпосередньо сприяє зростанню залученості громадян до електронних послуг та підвищенню їхньої задоволеності [48].

Запроваджувати змішані формати надання послуг, а саме, працювати над розробкою таких гібридних систем, що злучатимуть електронні сервіси із стаціонарними пунктами обслуговування (як-от ЦНАПи чи поштові відділення). У цих місцях фахівці матимуть змогу надавати необхідне

сприяння тим громадянам, у котрих відсутні цифрові компетентності, для освоєння та використання онлайн-інструментів. Такий підхід гарантує включеність і сприяє подоланню цифрової нерівності, забезпечуючи доступ до державних благ для всіх категорій населення, що повністю відповідає принципу «не лишати поза увагою жодної особи».

7) Розробити вдосконалену національну стратегію щодо даних.

Щоб мати змогу належно керувати даними та їх застосовувати, вкрай необхідно створити загальнодержавну концепцію оперування даними. Ця концепція мусить детально викладати принципи й настанови стосовно того, як дані збиратимуться, де зберігатимуться та яким чином використовуватимуться. Окрім того, ця стратегія повинна охоплювати положення, що регулюють як саме керування цими даними, так і захист приватності, пов'язаної з ними.

Інформаційне суспільство, це в першу чергу економічна система, де головним активом є знання. Однак, якщо ставити перед нею вузькоспрямовану мету – лише забезпечити функціонування сектору, базованого на знаннях (економіки), – вона неминуче зазнає швидкого краху. Сфера інформаційно-комунікаційних технологій, безумовно, становить ядро так званої «нової економіки». Проте, важливо пам'ятати, що просте убезпечення розвитку лише інформаційної інфраструктури не здатне спричинити глибинні трансформації, необхідні для формування інформаційного суспільства. Усе це є єдиною системою, тому інклюзивний прогрес можливий лише через інтеграцію ІКТ-сектору в цю систему та його зв'язок з іншими галузями економіки, численними взаємопов'язаними ланцюгами інформатизації та усіма сферами життя громади.

З огляду на це, розбудова суспільства, заснованого на знаннях, в Україні мусить спиратися на комплексний підхід. Він повинен охоплювати стратегічне бачення сфери суспільної інформації, визначення чітких пріоритетів у галузі знань та органічну інтеграцію у наявне соціально-економічне, політичне та

соціокультурне середовище. Увесь цей процес має ґрунтуватися суворо на національних засадничих засадах, а також на передових міжнародних здобутках, що стосуються економічного зростання та національного розвитку [94].

3.3. Прогнозні оцінки та очікувані соціально-економічні ефекти від вдосконалення державної політики в інформаційній сфері

Покращення державної політики стосовно інформаційного суспільства та електронного урядування (е-урядування) в Україні, узгоджене з європейськими нормами, спричинить суттєві й різноманітні соціально-економічні наслідки. Розрахунки, зроблені наперед, спираються на практику держав Європейського Союзу та можливості цифрової трансформації [117].

Передбачається, що вдосконалення цієї політики сприятиме збільшенню валового внутрішнього продукту, зміцненню конкурентних позицій та раціоналізації державних фінансових витрат.

Таб.3.

Напрямок	Прогнозна оцінка та (3–5 років)	Обґрунтування
Зростання ВВП за рахунок ІКТ	Додатковий приріст 1–1.5% ВВП щорічно.	Стимулювання цифрової економіки, зростання інвестицій у цифрову інфраструктуру та IT-сектор, підвищення продуктивності праці за рахунок автоматизації.
Економія Державних Витрат	10–15% економії на адміністративних та логістичних витратах органів влади.	Перехід на безпаперовий документообіг, оптимізація штату, зменшення необхідності у фізичних офісах, реалізація принципу Once-Only Principle.
Інвестиційна привабливість	Зростання прямих іноземних інвестицій у цифрову інфраструктуру та IT-сектор на 20–30%.	Гармонізація із законодавством ЄС (GDPR, кібербезпека) знижує ризики для іноземних інвесторів та збільшує довіру.

Скорочення часу на бізнес-процедури	Зменшення часу на реєстрацію бізнесу, отримання дозволів тощо, на 50–70%.	Повна цифровізація та реінжиніринг послуг "за життєвими подіями", відсутність фізичного контакту з чиновником.

Таб.3. Прогнози щодо вдосконалення державної політики в інформаційній сфері

Очікується, що соціальні наслідки матимуть свій фокус на покращенні добробуту, забезпеченні прозорості та зміцненні віри у державні установи. Увесь спектр адміністративних послуг, які піддаються цифровізації, цілодобово, сім днів на тиждень, будуть реалізовані в електронному форматі. Це має ключове значення для громадян, які мешкають у віддалених місцевостях та сільській місцевості, оскільки це суттєво зменшить їхні витрати часу та коштів на комунікацію з органами влади. Масштабні освітні ініціативи та впровадження змішаних форматів обслуговування призведуть до суттєвого скорочення розриву у цифровізації. Передбачається, що частка громадян, обізнаних із цифровими технологіями, сягне позначки у 75–80 відсотків [22].

Прозорість набуде більшого розмаху, а корупція на побутовому рівні зменшиться, що стане наслідком автоматизації механізмів прийняття рішень та усунення людського втручання із рутинних операцій (таких як видача довідок чи здійснення реєстрації). Очікується розширення переліку публічних державних реєстрів та масивів інформації, що, своєю чергою, підсилить можливості громадського моніторингу та послужить підґрунтям для розробки нових інноваційних рішень (наприклад, у сфері антикорупційних розслідувань).

Участь громадян посилиться, зокрема, електронна демократія (e-Democracy) отримає новий поштовх. Це стимулюватиме розвиток засобів для електронних петицій, консультаційних процедур та голосувань, що підвищить рівень залученості населення до формування рішень та забезпечить більшу відповідність державної політики суспільним запитам [94].

Удосконалення політики є життєво важливим для гарантування безпеки держави та злагодженої роботи органів влади.

Кардинальне посилення кіберзахисту об'єктів критичної інформаційної інфраструктури (енергетичний сектор, фінансові установи, транспортні мережі). Передбачається, що час, потрібний для реагування на кіберзагрози, скоротиться удвічі, а також зменшиться потенційна фінансова шкода від успішних атак. Довіра до державних реєстрів та даних, що в них містяться, підвищиться внаслідок впровадження уніфікованих критеріїв безпеки та механізмів дублювання даних [109].

Ефективність державного управління матиме за мету перенаправлення зекономлених організаційних ресурсів на найважливіші соціальні ініціативи та пожвавлення економічної діяльності.

Таким чином, попередні розрахунки демонструють, що послідовне покращення державної стратегії у контексті інформаційного суспільства та електронного урядування слугує потужним рушієм для тривалого економічного розвитку та становлення демократичних інститутів в Україні. Передбачувані наслідки сягають значно глибше, ніж просто технічні аспекти, формуючи державу, яка є ефективною, відкритою для контролю та орієнтованою на потреби громадян.

Висновки до розділу 3

Дослідження сфокусовано на способах покращення державної стратегії в питанні інформаційного суспільства на теренах України, окреслює всеосяжний метод для оновлення та розбудови цієї життєво значущої сфери, завважуючи на здобутках Європи та встановлюючи певні стратегічні напрямки.

Стосовно стратегічного вдосконалення та інтеграції з Європою, було констатовано потребу підлаштувати державну політику під європейські норми та передові приклади. Наріжний камінь закладено у комплексному рішенні,

яке охоплює перебудову системи управління, підвищення цифрової обізнаності громадян та забезпечення захисту інформаційних активів. Першочергові завдання – це електронне урядування, розбудова інфраструктури широкосмугового зв’язку та забезпечення кібербезпеки.

З метою покращення стану інфраструктури та ресурсного забезпечення, виокремлено низку цілеспрямованих заходів. Вони стосуються оновлення телекомунікаційних мереж, об'єднання державних інформаційних баз даних (формування спільного цифрового середовища), а також гарантування сталості та відкритості доступу до цих ресурсів. Акцентується увага на потребі формування сприятливих законодавчих умов для розвитку інновацій у сфері ІКТ, залучення капіталу, допомоги новоствореним підприємствам (стартапам) та вдосконалення підготовки фахівців (освіта у сфері ІТ). Усе це має слугувати каталізатором для економічного піднесення.

Щодо очікуваних результатів, то реалізація запропонованих кроків має потенціал принести вагомі соціально-економічні вигоди. Передбачається, що настане зростання дієвості органів влади (зокрема, через зниження рівня корупції та прискорення надання сервісів), підвищиться здатність економіки конкурувати завдяки бурхливому розвитку ІКТ-сфери, а якість життя населення покращиться завдяки ширшому доступу до електронних сервісів та зростанню рівня їхньої цифрової обізнаності.

Таким чином, модернізація державної стратегії у сфері інформаційного суспільства для України – це невід'ємна умова євроінтеграційних прагнень, економічного розвитку та формування держави, яка є дієвою, відкритою та відповідає сучасним вимогам. Ключ до успіху полягає у всеосяжному застосуванні запланованих дій: від розбудови технічної бази та об'єднання наявних потужностей до стимулювання новаторства та освітньої підготовки громадян.

ВИСНОВКИ

У кваліфікаційній роботі представлено теоретичне підсумування та сучасне розв'язання нагальної наукової проблеми, яка полягає у доведенні обґрунтованості як теоретичних, так і практичних сторін державної стратегії стосовно інформаційного суспільства в України. Завдання поставлене в рамках цього дослідження було реалізовано, і ключові етапи виконано. Аналіз, проведений у ході цієї роботи, дав змогу сформулювати наступні положення.

1. У межах виконання поставленого завдання, а саме – у рамках систематизації та акцентування уваги на ключових теоретичних положеннях, суті та особливостях інформаційного суспільства та відповідних державних заходів, було здійснено поглиблений розгляд наукової бази. Було уточнено, що під інформаційним суспільством (ІС) розуміється наступний етап розвитку соціуму, де здобутки знань та інформаційні потоки виступають у ролі головного дійового (економічного) активу, а різноманітні інформаційно-комунікаційні технології (ІКТ) стають провідним засобом для змін у соціальній, економічній та політичній сферах. Встановлено, що ІС властиві такі ознаки, як всеохоплююча глобалізація, побудова на мережевих принципах, пріоритетність сфери послуг та високий ступінь підготовленості (освіченості) населення.

Систематизовано основні наукові погляди на сутність ІС (як технічний, фінансово-господарський, суспільно-культурний, територіальний аспекти), що дало змогу скласти цілісне уявлення про цей суспільний устрій, оминаючи спрощені тлумачення. Окрім того, встановлено, що державний курс у сфері ІС являє собою сукупність завдань, засад та інструментів, націлених на створення передумов для переходу до ІС і посилення його позитивних сторін (збільшення прибутків, поширення народовладдя, покращення побуту) та зменшення загроз (розрив у доступі до технологій, захист відомостей). Основними напрямами такого курсу є розбудова мереж зв'язку та обробки

інформації, формування електронного урядування, цифрова підготовка громадян та забезпечення кіберзахисту.

Таким чином, повністю завершено роботу з упорядкування та конкретизації теоретично-методологічного підґрунтя, що слугує обов'язковою засадою для наступного дослідження процесу розробки й упровадження державної політики у галузі інформаційного суспільства.

2. Здійснивши аналіз та підсумувавши зарубіжний досвід щодо розробки й впровадження державної стратегії у цифровізаційній царині (зокрема, провівши огляд скандинавського, англосаксонського, азійського підходів та практик країн Євросоюзу), ми дійшли розуміння, що кожна держава вирізняється власними рисами еволюції, особливо це стосується й питань, пов'язаних із формуванням інформаційного соціуму. Ми дослідили ключові системи та їхні індивідуальні риси, аби з'ясувати, який саме підхід є найбільш оптимальним для України.

Огляд міжнародного досвіду дає змогу виявити низку загальних, а також пристосовних моментів, які є вирішальними для українського курсу на цифровізацію: 1) зразкові моделі Скандинавії чи Сінгапуру доводять слушність настанови, що єдиний координуючий орган (подібний до українського Мінцифри) мусить володіти вагомими повноваженнями для забезпечення уніфікації та реалізації рішень у межах усіх гілок влади; 2) жодна цифрова трансформація не здійсниться без розгалуженого доступу до високошвидкісного мережевого з'єднання та надійної, універсальної системи електронного посвідчення особи (подібної до BankID у Північній Європі чи національних e-ID програм); 3) найкращі практики показують, що правова база повинна бути еластичною та індиферентною до конкретних технологій, за мету маючи не стримувати, а заохочувати появу нового. Надзвичайно важливим є оперативне зняття нормативних перепон для надання цифрами послуг; 4) у країнах Європи та Скандинавії ключовим елементом вважається

довіра населення. Для її зміцнення застосовуються механізми захисту особистих даних (за зразком GDPR) та суттєве нарощування кіберзахисту.

Отже, міжнародний досвід слугує доказом того, що Україна обрала вірний напрямок, концентруючи зусилля на формуванні уніфікованого цифрового хабу (у вигляді Мінцифри) та ключового програмного продукту («Дія»). Цей підхід є вдалим синтезом сервісно-орієнтованої моделі, притаманної англосаксонським країнам, та скандинавського прагнення до повноцінної інтеграції державних сервісів. Проте, для забезпечення подальшого прогресу життєво необхідним є стабільне та достатнє фінансування, прискорення процесу приведення національного законодавства у відповідність до стандартів ЄС, екстенсивне впровадження успішних рішень у регіонах, а також безперервне зміцнення кібероборони об'єктів критичної інфраструктури.

3. Дослідивши розвиток та сьогодення правового й інституційного підґрунтя державної політики щодо інформаційного суспільства та цифровізації в Україні, ми констатуємо: українське законодавство еволюціонувало від поодиноких заходів з інформатизації до становлення цілісної, хоча й ще не остаточно оформленої, системи регулювання цифровізації та електронного врядування. На старті домінували технічні аспекти, тоді як нині увага зосереджена на перетворенні державних послуг, кіберзахисті та імплементації передових технологій («Дія»). Проте, попри суттєвий поступ, нормативно-правове поле все ще демонструє певну розрізненість. Спостерігається явище колізій між нещодавніми цифровими законами та застарілими нормативними актами, що сповільнює стрімке та продуктивне впровадження цифрових інструментів. Нагальною потребою є гармонізація та систематизація законодавчих положень.

Структура інституцій зазнала значних трансформацій, головним чином через формування Міністерства цифрової трансформації (Мінцифри) як головного координуючого органу політики. Такий крок сприяв консолідації

спрямованих зусиль. Проте, нагальною є необхідність у зміцненні взаємодії між Мінцифри, рештою центральних органів державної влади та органами місцевого самоврядування, аби гарантувати послідовність у реалізації державної політики.

Область, де спостерігається певна вразливість, це здатність до впровадження задуманого. Нерідко бракує докладно пропрацьованих вторинних нормативних документів, які є життєво необхідними для введення в дію ухвалених базових законів. На додаток до цього, людський ресурс та матеріально-технічна база на рівні громад та у деяких державних структурах не завжди спроможні забезпечити виконання амбітних планів щодо цифровізації.

Робота над законодавчою базою досить динамічно рухається у напрямі євроінтеграції та приведення національних норм у відповідність до права ЄС, зокрема це стосується питань кібернетичної безпеки, збереження особистої інформації та питань електронної ідентифікації. Такий розвиток подій варто розцінювати як позитивний зсув на шляху до досягнення взаємодії з європейським цифровим простором.

З огляду на проведене дослідження, можна зробити висновок, що для України відкриваються широкі можливості щодо доведення до кінця процесу становлення інформаційного суспільства та здійснення успішних кроків у цифровій трансформації. Проте реалізація цього потенціалу вимагає ретельного вдосконалення чинного законодавчого поля та посилення інституційних структур, насамперед у площинах фінансового забезпечення, комплектування кваліфікованими фахівцями та забезпечення належного моніторингу виконання намічених стратегічних планів.

4. Здійснивши ретельне вивчення того, як уряд втілює у життя головні свої засади, серед яких розбудова електронного урядування, гарантування кіберзахисту та зменшення цифрового нерівності, констатуємо: Україна здобула вагомі досягнення у сфері електронного врядування. Це стало

можливим завдяки запуску провідних цифрових рішень, а саме мобільного додатку «Дія» та відповідного порталу. Такий крок дозволив безпрецедентно динамічно перевести державні послуги у віртуальний простір, суттєво покращивши громадянам можливість користуватися адмінпослугами. Впроваджено електронні версії документів (посвідчення особи, водійське посвідчення, «ковідні» сертифікати), які набули чинності згідно із законом, а також розпочато інтеграцію державних реєстрів шляхом використання платформи «Трембіта». Усе це створює підґрунтя для постачання послуг, згрупованих за життєвими обставинами.

Незважаючи на досягнення, все ж таки залишається питання невеликої якості та недостатньої сучасності відомостей у певних основних регістрах, а також незавершеного приєднання усіх державних структур до уніфікованих інфосистем. Це сповільнює повний рух до концепції «держава як сервіс».

Щодо кіберзахисту, ми бачимо інституційне посилення та прийняття низки ключових законодавчих актів, націлених на охорону життєво важливої інформаційної інфраструктури. Було сформовано Національний орган координації з питань кібербезпеки, а повноваження Держспецзв'язку розширено.

Фактичне втілення у життя визначеної політики засвідчило спроможність держави швидко давати відсіч масштабним кібернападам, котрі особливо активізувалися внаслідок зовнішньої ворожої діяльності. Цей факт свідчить про достатньо високу міцність системи державного захисту в кіберпросторі.

Проте, досі не вирішеним питанням є недостатня обізнаність щодо кібергігієнічних норм та відсутність належного захисту у значної кількості представників приватного бізнесу та на рівні місцевих (регіональних) урядів, які не належать до кола безпосередніх об'єктів критичної інформаційної інфраструктури, що породжує ймовірні слабкі місця для усієї системи загалом.

Вживаються заходи задля мінімізації розбіжностей у цифровому доступі, головним чином завдяки ініціативам, спрямованим на забезпечення доступу до високошвидкісного мережевого з'єднання для об'єктів, важливих для суспільства (наприклад, освітніх та медичних закладів), а також для поселень, розташованих далеко. Це стимулює розширення охоплення цифровими технологіями.

Головною проблемою залишається різниця у розвитку між регіонами. Можливості отримання доступу до необхідної інфраструктури та рівень володіння цифровими навичками значно вар'юються, якщо порівнювати урбанізовані центри та сільські території. Для повного усунення цієї розбіжності потрібні вагомі фінансові інвестиції та спеціально розроблені регіональні програми.

Отже, втілення державної політики на практиці засвідчує помітний поступ у сфері електронного урядування, значну гнучкість у питаннях кіберзахисту, а також започаткування планомірної діяльності стосовно усунення цифрової нерівності. Проте, аби Україна могла досягти повної цифрової зрілості, їй слідує сфокусувати увагу на впорядкуванні якості інформації, що міститься у реєстрах, розширенні заходів кіберзабезпечення на усі ешелони влади та зменшенні помітних відмінностей між регіонами щодо доступу до технічних засобів та цифрових навичок.

5. Виявивши основні проблеми, недоліки та бар'єри, що заважають належному втіленню державної політики у сфері інформаційного суспільства в Україні, ми дійшли переконання, що головні обмежувальні чинники полягають у наступному:

- Хоча Міністерство цифрової трансформації й було засноване, наявність розпорошеності повноважень та слабкої злагоди між основними державними виконавчими відомствами все ще помітна. Це спричиняє дублювання робочих функцій, несинхронізованість стратегічних намірів та уповільнене запровадження уніфікованих норм.

- Багато державних інституцій демонструють інертність та небажання приймати цифрові інструменти. Це зумовлено недостатністю потрібного стимулу, звичною прихильністю до застарілих робочих процесів, а також недостатність цифрових навичок у вищого керівництва.

- Серйозною перешкодою на шляху до функціонального електронного урядування є те, що інформація у важливих державних реєстрах є низької якості, не відповідає дійсності або ж зберігається фрагментовано. Через це стає неможливим пропонувати комплексні сервіси, згруповані навколо «життєвих обставин», і змушує вдаватися до постійних ручних звірок даних.

- Надходження фінансових ресурсів з державного бюджету для цифрових ініціатив, зокрема на рівні областей та громад, часто не відповідають тим високим цілям, що окреслені у стратегічних планах. Залежність від коштів, що надходять від закордонних партнерів, несе загрозу для довгострокової життєздатності проєктів.

- Критично гостро стоїть питання нестачі фахівців ІТ-сфери з високою кваліфікацією та управлінців цифровими процесами у державних установах, що зумовлене нездатністю пропонувати конкурентні заробітні плати на тлі приватного сектору. Це сповільнює як створення нових, так і забезпечення функціонування комплексних цифрових платформ.

- Велика частка технічного забезпечення (апаратного та програмного), особливо поза столицею, є вже давно неактуальною як щодо технологій, так і щодо фізичного стану, що відкриває можливості для кібератак та унеможливлює ефективну роботу з великими обсягами інформації.

- Незважаючи на посилення заходів із кібербезпеки на центральному рівні, загроза кібератак залишається вагомою, особливо з огляду на зовнішню агресію, а вразливість певних регіональних інформаційних систем може спричинити «слабке місце» у загальній архітектурі безпеки.

- Все ще присутній суттєвий розрив у цифровізації між міськими та сільськими районами, що стосується як доступу до високошвидкісного

інтернету, так і рівня цифрових навичок громадян, що слугує бар'єром для забезпечення рівноправного доступу до цифрових сервісів.

- У певних прошарках населення досі спостерігається низька довіра до державних електронних платформ (зокрема, у контексті захисту персональної інформації), що гальмує їхнє широке впровадження.

З огляду на виявлені труднощі, стає очевидним, що для спроможності рухатися далі від етапу тестування проєктів до сталої та всеохоплюючої цифровізації, нагально потрібна глибока перебудова (реформа) у сферах управління, людських ресурсів та фінансового забезпечення. Така реформа має бути націлена на усунення опору змінам, притаманного установам, та забезпечення надійного захисту від загроз (кіберстійкості) для всієї сукупності державних інформаційних систем.

6. Розробивши конкретні науково-практичні рекомендації та обґрунтувавши шляхи удосконалення державної політики для збільшення дієвості та прискорення зближення з Європою, ми дійшли переконання, що подальше успішне просування цифрових змін в Україні обумовлене послідовним здійсненням таких першочергових дій:

1) Слід уніфікувати основні законодавчі акти у сфері цифровізації та якнайшвидше привести їх у відповідність до правової бази ЄС у цій галузі. Такий захід гарантуватиме правову прозорість та технічну взаємосумісність із Європейським Єдиним цифровим ринком.

2) Забезпечити міцнішу інституційну узгодженість. У цьому контексті Міністерству цифрової трансформації (як провідному органу) потрібно надати чітко визначені та розширені повноваження, аби воно могло стандартизувати та зробити обов'язковою інтеграцію усіх державних інформаційних ресурсів. Це має бути підкріплено наданням фінансових та наглядових механізмів, необхідних для подолання розрізненості між відомствами.

3) Впровадити постулат «одноразового подання» (one-time only concept): необхідно законодавчо оформити та гарантувати беззаперечне виконання

принципу подачі даних лише один раз, використовуючи високоякісні та сумісні реєстри, що є наріжним каменем вимог ЄС до функціонування електронного урядування.

4) Оновити реєстри, що стосуються якості даних. Головний акцент слід зробити на перевірці, очищені й підтримці завжди актуального стану інформації у ключових державних базах даних. Варто запровадити уніфікований спосіб перевірки даних у момент їх внесення, а також заохочувати впровадження хмарних рішень (пріоритет хмари) задля більшої адаптивності та скорочення витрат на обслуговування.

5) Посилити заходи кіберзахисту. Треба поширити застосування норм кібербезпеки та вимог, призначених для захисту життєво важливих інформаційних систем, на системи, що використовуються на рівні областей та громад. Для цього потрібні додаткові фінансові вливання та централізована технічна підтримка.

6) Здійснити трансформацію кадрової політики: імплементувати гнучкі та привабливі схеми винагороди та методи притягнення ІТ-спеціалістів на держслужбу. Одночасно із цим, необхідно запровадити обов'язкове навчання основам цифрових технологій для всіх представників державних органів, незалежно від посади.

7) Ліквідувати цифрову нерівність: посилити державні ініціативи, спрямовані на забезпечення надійного широкосмугового доступу до мережі Інтернет у сільських та важкодоступних районах. Також варто розширити навчальні курси з цифрової обізнаності, роблячи їх релевантними для потреб різноманітних соціальних прошарків.

Отже, ці розроблені рекомендації окреслюють для України шлях, який дасть змогу укріпити вже здобуте у сфері електронного урядування, усунути найважливіші інституційні перешкоди й пришвидшити входження до Єдиного цифрового ринку Євросоюзу. Наполегливе втілення цих заходів є життєво

необхідною передумовою для зростання дієвості державного адміністрування та формування міцного, відкритого для всіх інформаційного соціуму.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналіз бар'єрів цифрової трансформації в Україні : звіт проєкту USAID/UK aid «Прозорість та підзвітність у державному управлінні та послугах/TAPAS». Київ, 2023. 120 с.
2. Антонова Л. В. Цифрова нерівність як соціальна проблема інформаційного суспільства. *Інвестиції: практика та досвід*. 2021. № 4. С. 98–103.
3. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти. Харків : Вид-во НУВС, 2019. 240 с.
4. Баранов О. А. Державний механізм управління в інформаційній сфері : правові аспекти. *Інформація і право*. 2018. № 3 (26). С. 112–124.
5. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи : монографія. Київ : Вид. дім «КМ Академія», 2015. 316 с.
6. Белл Д. Постіндустріальне суспільство, що народжується. Прогноз соціального розвитку. Київ : Основи, 2003. 580 с.
7. Бєляков К. І. Інформатизація в Україні: проблеми правового регулювання. *Право та інновації*. 2023. № 1. С. 40–47.
8. Бєляков О. О. Інформаційне суспільство: світовий досвід та українська перспектива. Київ : КНТ, 2021. 256 с.
9. Бєляєва Н. В. Соціально-політичний маркетинг у системі державного управління. *Грані*. 2021. Т. 24, № 9. С. 540–548.
10. Біньсін Ф. Кіберпростір та цифровий суверенітет : наук. вид. / пер. з англ. Київ : Наукова думка, 2023. 312 с.
11. Братко І. В. Інформаційне перевантаження як чинник трансформації когнітивної сфери особистості. *Психологічний часопис*. 2020. № 6 (4). С. 15–24.
12. Брижко В. М. Цифрове право: реалії та перспективи. *Інформація і право*. 2023. № 1. С. 10–18.

13. Вебер А. С. Державна політика в інформаційному суспільстві: виклики та можливості. *Стратегічні пріоритети*. 2022. № 1. С. 45–52.

14. Вебстер Ф. Теорії інформаційного суспільства / пер. з англ. В. Білецький. Київ : Обізнаність, 2013. 452 с.

15. Глобальні ризики та кібербезпека в умовах цифровізації : монографія / за ред. В. А. Ліпкана. Київ : Ліпкан В. А., 2022. 480 с.

16. Гурковський В. І. Теоретико-методологічні засади державної політики інформатизації. *Державне управління: теорія та практика*. 2019. № 2. URL: http://nbuv.gov.ua/UJRN/Dutp_2019_2_5 (дата звернення: 12.10.2025).

17. Данильян О. Г. Правове регулювання інформаційних відносин : монографія. Харків : Право, 2021. 250 с.

18. Дафф А. С. Інформаційне суспільство: соціологічний підхід. Львів : Кальварія, 2005. 210 с.

19. Дзьобань О. В. Філософія інформаційного права : монографія. Харків : Право, 2018. 360 с.

20. Дубов Д. В. Кіберпростір як новий об'єкт державної політики. Київ : НІСД, 2016. 324 с.

21. Жиляєв І. В. Правове забезпечення цифрової трансформації України : монографія. Київ : Парламентське вид-во, 2022. 356 с.

22. Жиляєв І. В. Стан та проблеми розвитку інформаційного суспільства в Україні. *Інформація і право*. 2021. № 2 (37). С. 45–56.

23. Жиляєв І. В. Інформаційне суспільство: проблеми правового регулювання : монографія. Київ : Парламентське вид-во, 2018. 320 с.

24. Звіт про розвиток цифрової економіки України за 2023 рік / Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/storage/uploads/files/news_file/report_2023.pdf (дата звернення: 22.11.2025).

25. Інформаційне суспільство в Україні: стан, проблеми, перспективи : доп. Нац. комісії, що здійснює держ. регулювання у сфері зв'язку та інформатизації. Київ, 2024. 64 с.

26. Європейська Комісія. План дій з електронного урядування на 2016-2020 роки. URL: https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020

27. Карпенко О. В. Державне управління в умовах цифровізації: виклики та пріоритети : монографія. Київ : ІДУ НАН України, 2022. 256 с.

28. Карпенко О. В. Електронне урядування та державна політика : навч. посіб. Київ : ІДЕЯ ПРИНТ, 2020. 212 с.

29. Кастельс М. Інформаційна епоха: економіка, суспільство та культура / пер. з англ. А. П. Рябова. Київ : Ніка-Центр, 2006. 604 с.

30. Кастельс М. Становлення суспільства мережевих структур. Інформаційна епоха: економіка, суспільство та культура. Київ : Ніка-Центр, 2007. С. 15–78.

31. Когут Ю. І. Кібербезпека та сучасні загрози інформаційному суспільству. Київ : Кондор, 2022. 210 с.

32. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр.

33. Концепція розвитку штучного інтелекту в Україні : схвалена розпорядженням Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р.

34. Копилов В. А. Інформаційне право : підручник. Київ : Академія, 2020. 415 с.

35. Кормич Б. О. Інформаційне право : підручник. Одеса : Юридична література, 2018. 320 с.

36. Кудрявцева А. М. Електронне урядування як інструмент модернізації державного управління. *Ефективність державного управління*. 2023. Вип. 2 (75). С. 112–118.

37. Кушакова-Семенецька Н. Ю. Право на доступ до інформації в умовах глобалізації. *Юридичний науковий електронний журнал*. 2022. № 5. С. 130–133.

38. Левитін Д. Путівник по брехні. Критичне мислення в епоху постправди / пер. з англ. О. Осмоловської. Київ : Наш Формат, 2020. 256 с.

39. Ліпкан В. А. Інформаційна безпека України : навч. посіб. Київ : Кондор, 2018. 234 с.

40. Лютий Т. В. Культура інформаційного суспільства та цифрова ідентичність : монографія. Київ : Стилос, 2019. 312 с.

41. Макаренко Є. А. Міжнародні інформаційні відносини: цифрова дипломатія. Київ : Логос, 2021. 300 с.

42. Марущак А. І. Інформаційне право: доступ до інформації : навч. посіб. Київ : КНТ, 2019. 280 с.

43. Міжнародна інформаційна безпека: сучасні виклики та загрози / за ред. А. М. Кудрявцева. Київ : Центр навч. літ., 2019. 312 с.

44. Морозов А. Ю., Шуст Н. Б. Становлення інформаційного суспільства в Україні: виклики та перспективи. *Міжнародний науковий журнал «Дискурс»*. 2022. № 9 (417). URL: https://www.journal-discourse.com/uk/kataloh-statei/2022/2022-r-417-9/stanovlennia-informatsiinoho-suspilstva-v-ukraini-vyklyky-ta-perspektyvy.

45. Наслідки повномасштабного вторгнення РФ для телекомунікаційної галузі України : звіт Світового банку. 2023. 58 с.

46. Національна стратегія розвитку інформаційного простору України : проектні пропозиції. Київ : НІСД, 2024. 45 с.

47. Нестеренко О. В. Відкриті дані як інструмент прозорості державного управління. *Публічне управління та митне адміністрування*. 2021. № 2. С. 55–60.

48. Огляд стану цифровізації в Україні : аналітичний звіт / Міністерство цифрової трансформації України. Київ, 2024. 84 с.

49. Парізер Е. Filter Bubble: те, що інтернет приховує від вас / пер. з англ. К. Диса. Київ : Наш Формат, 2022. 240 с.

50. Петрик В. В. Інформаційна безпека держави : навч. посіб. Київ : КНТ, 2015. 248 с.

51. Плескач В. Л. Електронна комерція : підручник. Київ : Знання, 2017. 450 с.

52. Плєханов Д. А. Особливості державної політики Китаю в сфері інформаційних технологій. Східний світ. 2021. № 3. С. 88–94.

53. Полякова О. С. Цифровізація адміністративних послуг: виклики та переваги. *Державне будівництво*. 2021. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2021_1_12.

54. Почепцов Г. Г. Психологічні операції : навч. посіб. Київ : Вид. дім «Києво-Могилянська академія», 2015. 268 с.

55. Прайвасі у цифровому світі : філософсько-правовий аспект / за заг. ред. В. М. Тертишника. Дніпро : ЛІРА, 2021. 190 с.

56. Про авторське право і суміжні права : Закон України від 01.12.2022 № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20.

57. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17.

58. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19.

59. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15.

60. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20.

61. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр.

62. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17.

63. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

64. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20.

65. Про медіа : Закон України від 13.12.2022 № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20.

66. Про Національну програму інформатизації : Закон України від 01.12.2022 № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20.

67. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

68. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16.

69. Про розвиток електронних послуг та електронної ідентифікації : аналіт. доп. / за ред. О. В. Карпенка. Київ : Нац. ін-т стратег. дослідж., 2024. 48 с.

70. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021.

71. Про стан кібербезпеки в Україні та невідкладні заходи щодо її зміцнення : аналіт. зап. Київ : Нац. ін-т стратег. дослідж., 2023. 24 с.

72. Про стимулювання розвитку цифрової економіки в Україні : Закон України від 15.07.2021 № 1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20.

73. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 22.12.2025).

74. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету Міністрів України від 15.05.2013 № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-р.

75. Про хмарні послуги : Закон України від 02.02.2022 № 2046-IX. URL: https://zakon.rada.gov.ua/laws/show/2046-20.

76. Риженко О. В. Державна політика у сфері електронного урядування : теорія та практика. Київ : Логос, 2019. 288 с.

77. Світовий досвід формування інформаційного суспільства: уроки для України : аналіт. доп. / Нац. ін-т стратег. дослідж. Київ : НІСД, 2023. 56 с.

78. Свобода слова та право на забуття : аналітичний звіт щодо європейської практики. *Інформаційне право*. 2023. № 4. С. 22–30.

79. Семенченко А. І. Державне управління та державна політика в інформаційній сфері. Дніпро : ДРІДУ НАДУ, 2017. 244 с.

80. Семенченко А. І. Формування та реалізація державної політики в інформаційній сфері : монографія. Київ : Нац. акад. держ. упр. при Президентові України, 2022. 384 с.

81. Семенченко А. І., Дрешпак В. М. Державне управління та державна політика в інформаційній сфері : навч. посіб. Дніпро : ДРІДУ НАДУ, 2017. 244 с.

82. Сенор Д., Сінгер Ш. Країна стартапів. Історія ізраїльського економічного дива / пер. з англ. К. Диса. Київ : Yakaboo Publishing, 2016. 368 с.

83. Скулиш Є. Д. Інформаційна безпека в умовах гібридної війни. Київ : Наука, 2023. 270 с.

84. Соснін О. В. Інформатизація як чинник модернізації державного управління. *Стратегічні пріоритети*. 2020. № 3. С. 115–123.

85. Соснін О. В. Проблеми становлення інформаційного суспільства в Україні : навч. посіб. Київ : НАДУ, 2013. 352 с.

86. Стратегія цифрової трансформації соціальної сфери : схвалена розпорядженням Кабінету Міністрів України від 28.10.2020 № 1353-р. URL: https://zakon.rada.gov.ua/laws/show/1353-2020-р.

87. Ткачук А. Ф. Місцеве самоврядування та цифрова трансформація. Київ : ІКЦ, 2023. 140 с.

88. Тоффлер Е. Третя Хвиля / пер. з англ. А. Євса. Київ : Всесвіт, 2000. 480 с

89. Угода про асоціацію між Україною та Європейським Союзом. URL: https://zakon.rada.gov.ua/laws/show/984_011.

90. Федоров М. А. Пріоритети цифровізації України. *Офіційний вісник Мінцифри*. 2024. № 1. С. 5–12.

91. Хавронюк М. І. Проблеми та перспективи адаптації законодавства України до стандартів ЄС у сфері цифрових прав. *Право та інновації*. 2023. № 2 (42). С. 15–22.

92. Хантінгтон С. Зіткнення цивілізацій / пер. з англ. Н. Климчука. Київ : ПП «Вид-во Жупанського», 2019. 448 с.

93. Цап Т. О. Досвід Естонії у впровадженні електронного урядування: уроки для України. Науковий вісник Ужгородського національного університету. 2019. Вип. 24. С. 145–149.

94. Цифрова грамотність населення України : звіт за результатами загальнонаціонального дослідження / Міністерство цифрової трансформації України. Київ : МЦТ, 2023. 56 с.

95. Цифрова трансформація в умовах війни : звіт Міністерства цифрової трансформації України за 2022-2023 рр. URL: https://thedigital.gov.ua/storage/uploads/files/news_file/war_report.pdf.

96. Цимбалюк В. С. Правове забезпечення кібербезпеки: світовий досвід. *Юридична газета*. 2022. № 12. С. 14–16.

97. Черевко О. В. Інформаційне суспільство: поняття, ознаки, етапи формування. Право та державне управління. 2018. № 2. С. 45–51.

98. Чукут С. А. Теоретико-методологічні засади становлення та розвитку інформаційного суспільства. Інвестиції: практика та досвід. 2016. № 18. С. 104–109.

99. Шейко В. М. Культура. Інформація. Наука : монографія. Харків : ХДАК, 2011. 312 с.].

100. Швець М. Я. Державна інформаційна політика та право : монографія. Київ : Парламентське вид-во, 2018. 380 с.

101. 2030 Digital Compass: the European way for the Digital Decade. European Commission. Brussels, 2021. 25 p.

102. Being Digital. Negroponte N. New York : Knopf, 1995. 256 p.

103. Code: And Other Laws of Cyberspace. Lessig L. New York : Basic Books, 2006. 432 p.

104. Cybersecurity and Infrastructure Security Agency (CISA). Strategic Plan 2023-2025. URL: https://www.cisa.gov/strategic-plan (дата звернення: 22.12.2025).

105. Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. World Summit on the Information Society. Geneva, 2003. URL: https://www.itu.int/net/wsis/docs/geneva/official/dop.html (дата звернення: 22.12.2025).

106. Digital Government Index 2023. OECD. URL: https://www.oecd.org/governance/digital-government/digital-government-index.htm.

107. Digital India: Power to Empower. Ministry of Electronics and Information Technology, Government of India. URL: https://www.digitalindia.gov.in (дата звернення: 22.12.2025).

108. Dutton W. H. The Oxford Handbook of Information and Communication Technologies. Oxford : Oxford University Press, 2013. 640 p.

109. E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. United Nations. New York : UN, 2024. 280 p.

110. Ethics Guidelines for Trustworthy AI. High-Level Expert Group on Artificial Intelligence. European Commission, 2019. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (дата звернення: 22.12.2025).

111. Government Digital Service. The Government Digital Strategy. London : Cabinet Office, 2012. URL: https://www.gov.uk/government/publications/government-digital-strategy (дата звернення: 22.12.2025).

112. Global Cybersecurity Index 2024. ITU. Geneva : ITU, 2024. 110 p.

113. Larson J. F. The Race for 5G Supremacy: Why South Korea is Leading. International Journal of Communication. 2020. Vol. 14. P. 120–135.

114. Masuda Y. The Information Society as Post-Industrial Society. Washington, D.C. : World Future Society, 1981. 171 p.

115. Machlup F. The Production and Distribution of Knowledge in the United States. Princeton : Princeton University Press, 1962. 416 p.

116. Recommendation on the Ethics of Artificial Intelligence. UNESCO. Paris : UNESCO, 2021. 40 p.

117. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union. 2016. L 119. P. 1–88.

118. Reglament (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR). URL: https://zakon.rada.gov.ua/laws/show/984_008-16.

119. Republic.com 2.0. Sunstein C. R. Princeton : Princeton University Press, 2007. 272 p.

120. The Fourth Industrial Revolution. Schwab K. Geneva : World Economic Forum, 2016. 172 p.

121. The Rise of the Creative Class. Florida R. New York : Basic Books, 2019. 416 p.

122. The Third Wave. Toffler A. New York : Bantam Books, 1980. 560 p.

123. The Wealth of Networks. Benkler Y. New Haven : Yale University Press, 2006. 528 p.

124. World Development Report 2023: Digital Dividends. World Bank. Washington, DC : World Bank, 2023. 350 p.