

Чорноморський національний університет імені Петра Могили

(повне найменування вищого навчального закладу)

Навчально-науковий інститут післядипломної освіти

(повне найменування інституту, назва факультету (відділення))

Кафедра журналістики та політології

(повна назва кафедри (предметної, циклової комісії))

«Допущено до захисту»

Завідувачка кафедри журналістики та
політології

_____ Тетяна СИДОРЕНКО
“ ” _____ 2026 року

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти «бакалавр»

за освітньо-професійною програмою «Політологія»
зі спеціальності 052 Політологія

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ЇХ ВПЛИВ НА ПОЛІТИЧНИЙ ПРОЦЕС В СУЧАСНОМУ СВІТІ

Виконав: здобувач(ка) IV курсу групи 431з
Кравченко Діана Олександрівна

(підпис)

Науковий керівник:
доктор політичних наук, професор
кафедри журналістики та політології
Іванов Микола Семенович

(підпис)

Рецензент:
Доктор політичних наук, професор
Шевчук Олександр Володимирович

(підпис)

Засвідчую, що в цій кваліфікаційній
роботі немає запозичень із праць
інших авторів без відповідних посилань

Здобувач _____

Миколаїв – 2026 рік

ЗМІСТ

ВСТУП_____	3
РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ВПЛИВУ ІТ НА ПОЛІТИКУ_____	9
1.1. Концептуалізація "Інформаційних технологій" та "Політичного процесу" в умовах мережевого суспільства_____	9
1.2. Основні моделі та форми електронної демократії (e-Democracy)	13
1.3. Вплив Big Data та штучного інтелекту (AI) на суб'єктів політики	18
РОЗДІЛ 2. АНАЛІЗ ТРАНСФОРМАЦІЇ КЛЮЧОВИХ ПОЛІТИЧНИХ ІНСТИТУТІВ ТА ЯВИЩ_____	25
2.1. Зміни у політичній комунікації та виборчих кампаніях_____	25
2.2. ІТ як інструмент державного управління та підвищення прозорості_____	30
2.3 Новітні виклики: Дезінформація, "Ехо-камери" та Кіберзагрози	35
РОЗДІЛ 3. ПРАКТИЧНИЙ АНАЛІЗ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПОЛІТИЧНОМУ ПРОЦЕСІ УКРАЇНИ _____	43
3.1. Аналіз впровадження електронного врядування та його вплив на публічні послуги в Україні _____	44
3.2. Дослідження впливу соціальних мереж на формування політичного порядку денного в умовах воєнного стану_____	47
3.3. Виклики кібербезпеки та протидія дезінформації як елемент політичного процесу України_____	52
ВИСНОВКИ _____	59
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ _____	64
ДОДАТКИ_____	68

ВСТУП

Актуальність дослідження. Актуальність дослідження зумовлена кардинальною трансформацією архітектури сучасної політики під впливом тотальної цифровізації суспільних відносин. У ХХІ столітті інформаційні технології перестали виконувати роль виключно допоміжного інструментарію комунікації, натомість перетворившись на самостійний, визначальний чинник структурування політичного процесу. Глобальне поширення мережевих платформ призвело до виникнення нової політичної реальності, де швидкість трансляції смислів, доступ до великих даних та алгоритмічне управління увагою виборців стають головними ресурсами влади.

Традиційні інститути політичного посередництва, такі як класичні медіа та партійні структури, поступово втрачають монополію на формування суспільного порядку денного. Натомість виникає простір «цифрової демократії», який, з одного боку, створює безпрецедентні можливості для прямої політичної участі, мережевої мобілізації та прозорості державного управління. З іншого боку, технологічний прогрес породив нові системні ризики: цифровізація виборчих процедур робить їх вразливими до зовнішніх кібервтручань, а алгоритмізація соціальних медіа сприяє радикалізації суспільної думки через створення «інформаційних бульбашок» та ефект «ехо-камер».

Особливої ваги обрана тема набуває в контексті розвитку технологій штучного інтелекту та нейромереж, які дозволяють здійснювати мікротаргетинг з високим ступенем персоналізації, що фактично нівелює принципи рівності в інформаційному протиборстві. Для України, яка перебуває в епіцентрі глобального протистояння та стикається з масштабними гібридними загрозами в кіберпросторі, дослідження механізмів інформаційного впливу є питанням не лише наукового інтересу, а й національної безпеки.

Необхідність виявлення оптимального балансу між перевагами цифрової свободи та потребою у захисті демократичних інститутів від маніпулятивних впливів визначає запит на ґрунтовний політологічний аналіз даної проблематики. Це зумовлює вибір теми дипломної роботи та логіку побудови наукового пошуку в межах переддипломної практики.

Стан наукової розробки дослідження. Стан наукової розробки теми дослідження характеризується значним масивом теоретичних та емпіричних напрацювань, які можна розділити на кілька ключових напрямів.

Першу групу становлять фундаментальні праці, присвячені концептуалізації інформаційного суспільства та логіці розвитку мережевих структур. Серед закордонних дослідників визначальну роль відіграють роботи М. Кастельса, який першим детально описав трансформацію владних відносин під впливом цифрових комунікаційних мереж, а також концептуальні підходи Е. Чедвіка щодо гібридної медіасистеми та праці Ю. Габермаса в контексті трансформації публічної сфери.

Другий напрям охоплює дослідження прикладного характеру, орієнтовані на аналіз моделей електронного врядування, цифрової демократії та специфіки використання великих даних і штучного інтелекту в електоральних процесах. У цьому контексті вагоме значення мають наукові розробки вітчизняних та іноземних фахівців, які вивчають ризики алгоритмічного маніпулювання, виникнення феноменів «ехо-камер» та функціонування систем мікротаргетингу.

Третій напрям наукового дискурсу сформовано навколо проблем забезпечення інформаційної безпеки та кіберзахисту політичних інститутів в умовах гібридних загроз. Особливу групу джерел становлять праці сучасних українських дослідників, які аналізують трансформацію вітчизняного політичного процесу, досвід функціонування екосистеми цифрових послуг та особливості протидії деструктивним інформаційно-психологічним операціям в умовах воєнного стану.

Об'єкт дослідження - трансформація сучасного політичного процесу в умовах глобальної цифровізації та розвитку інформаційно-комунікативних технологій.

Предмет - інструментарій, закономірності та наслідки впливу новітніх інформаційних технологій на механізми функціонування політичної системи та електоральну поведінку в цифровому середовищі.

Мета дослідження полягає у системному науковому аналізі ролі інформаційних технологій у сучасному політичному процесі, виявленні специфіки їхнього впливу на зміну моделей політичної комунікації та розробці стратегій мінімізації маніпулятивних ризиків у цифровому просторі.

Завдання дослідження:

1. Здійснити концептуалізацію понять «інформаційні технології» та «політичний процес» в умовах мережевого суспільства.
2. Дослідити основні моделі та форми електронної демократії (e-Democracy) у сучасних політичних системах.
3. Проаналізувати вплив технологій Big Data та штучного інтелекту (AI) на суб'єктів політики.
4. Визначити особливості трансформації політичної комунікації та виборчих кампаній під впливом інформаційних технологій.
5. Охарактеризувати роль інформаційних технологій як інструменту державного управління та підвищення прозорості діяльності органів влади.
6. Проаналізувати новітні цифрові виклики політичного процесу, зокрема дезінформацію, феномен «ехо-камер» та кіберзагрози.
7. Дослідити особливості впровадження електронного врядування та його вплив на надання публічних послуг в Україні.
8. Визначити вплив соціальних мереж на формування політичного порядку денного в умовах воєнного стану.
9. Оцінити виклики кібербезпеки та механізми протидії дезінформації як важливий елемент сучасного політичного процесу України.

Методи дослідження. Для досягнення поставленої мети та розв'язання визначених завдань у роботі використано сукупність загальнонаукових та спеціальних методів політологічного аналізу.

Системний підхід дозволив розглянути цифровізацію як комплексний чинник, що трансформує всі рівні політичного процесу - від державного управління до індивідуальної електоральної поведінки, перетворюючи політичну сферу на цілісну цифрову екосистему.

Компаративний аналіз застосовано для порівняння стратегій впровадження інформаційних технологій у розвинених демократіях (зокрема США та країнах ЄС) та особливостей цифрової трансформації політичної сфери в сучасних українських реаліях.

Структурно-функціональний метод допоміг класифікувати новітні ІТ-інструменти, такі як соціальні медіа, алгоритми штучного інтелекту та системи Big Data, за їхнім функціональним призначенням у процесах політичної комунікації та мобілізації.

Використання кібернетичного підходу сприяло вивченню механізмів зворотного зв'язку та алгоритмічного керування інформаційними потоками в мережевому середовищі.

Також, у дослідженні застосовано методи контент-аналізу цифрового контенту та івент-аналізу для вивчення практичних кейсів використання цифрових платформ під час виборчих кампаній.

Прогностичний метод дозволив окреслити перспективи розвитку електронної демократії та можливі сценарії протидії цифровому авторитаризму і маніпулятивним впливам.

Теоретичну базу роботи становлять фундаментальні праці провідних українських та закордонних дослідників у галузі політичної комунікативістики, теорії інформаційного суспільства та мережевої політики, зокрема концепції М. Кастельса, Е. Чедвіка та розробки вітчизняних науковців щодо проблем електронного урядування та інформаційної безпеки, що

дозволило забезпечити об'єктивність, наукову валідність та комплексність отриманих результатів.

Наукова новизна роботи полягає у тому, що вона є комплексним дослідженням трансформації політичних інститутів та процесів під впливом новітніх інформаційних технологій, що дозволило по-новому оцінити динаміку сучасної політичної суб'єктності.

Наукова новизна бакалаврської роботи полягає у тому, що:

вперше: здійснено комплексний аналіз впливу алгоритмізації та систем штучного інтелекту на процеси прийняття політичних рішень, що дозволило визначити концепцію «алгоритмічної політики» як нового етапу розвитку цифрової демократії; обґрунтовано роль великих даних (Big Data) не лише як технічного інструментарію, а як самостійного політичного ресурсу, що змінює баланс сил між державними та недержавними акторами в глобальному політичному просторі.

удосконалено: поняття «цифровізація політичного процесу», яке трактується як системне переформатування політичної реальності, де інформаційні технології стають визначальним чинником формування легітимності, мобілізації громадян та функціонування владних ієрархій; класифікацію інформаційних технологій політичного впливу, до якої включено механізми формування «інформаційних бульбашок», системи предиктивної аналітики електоральної поведінки та методику цифрового мікротаргетингу в умовах фрагментації публічної сфери.

дістало подальшого розвитку:- дослідження феномену «цифрового авторитаризму» та механізмів використання ІТ для посилення державного контролю, що дозволило окреслити межу між технологічним сприянням демократії та загрозами кібербезпеці політичних інститутів; стратегічні підходи до адаптації політичної системи України до викликів четвертої промислової революції через розвиток е-урядування, законодавче регулювання цифрових платформ та зміцнення інформаційної стійкості суспільства в умовах гібридних загроз.

Практичне значення роботи полягає у можливості використання висновків дослідження політичними консультантами та виборчими штабами для розробки стратегій комунікації в цифровому середовищі.

Результати дослідження також можуть бути корисними для викладачів та студентів у межах вивчення навчальних дисциплін «Теорія політичних партій та виборчих систем» та «Політична психологія».

Дипломна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

Зокрема, у першому розділі висвітлено теоретико-методологічні засади дослідження, а також розкрито сутність базових концепцій електронної демократії (e-Democracy), електронного урядування (e-Government) та специфіку впливу великих даних (Big Data) на політичну сферу.

Другий розділ присвячено комплексному аналізу трансформації ключових політичних інститутів та явищ, де особливу увагу приділено змінам у політичній комунікації, управлінні, а також новітнім викликам, таким як дезінформація та кіберзагрози.

У третьому розділі представлено практичний складник дослідження, який містить кейс-стаді українського досвіду цифровізації, емпіричний контент-аналіз впливу мережі Telegram на політичні процеси, а також обґрунтовані рекомендації щодо оптимізації безпекового та ефективного використання інформаційних технологій у сучасній політиці. Повний обсяг дипломної роботи налічує 72 сторінки, список використаних джерел містить 60 найменувань.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ВПЛИВУ ІТ НА ПОЛІТИКУ

1.1. Концептуалізація "інформаційних технологій" та "політичного процесу" в умовах мережевого суспільства

Теоретичне осмислення трансформації сучасної політичної реальності потребує першочергового переосмислення та операціоналізації її базових складників, якими є «інформаційні технології» (ІТ) та «політичний процес». В умовах становлення глобального інформаційного простору ці категорії втрачають свій класичний, лінійний зміст і набувають нових системних характеристик, зумовлених переходом людства до мережевої логіки організації суспільного буття. Фундаментом для розуміння цих фундаментальних змін є концепція мережевого суспільства, детально обґрунтована у працях соціолога М. Кастельса. Дослідник переконливо доводить, що нова соціальна структура базується на мережах, які управляються за допомогою цифрових інформаційно-комунікаційних технологій, що радикально змінює механізми генерування, розподілу та використання влади в соціумі [15].

Відтак, інформаційні технології перестають бути просто технічним інструментом передачі даних, перетворюючись на визначальне середовище, у якому формуються, функціонують та еволюціонують сучасні політичні інститути.

У межах наукового дискурсу поняття «інформаційні технології» традиційно трактується як сукупність взаємопов'язаних наукових, технологічних та інженерних дисциплін, що вивчають методи ефективної організації праці людей, зайнятих обробкою, передачею та зберіганням інформації. Проте в контексті політичної науки ключову роль відіграє не технічний, а саме соціополітичний аспект ІТ. Як зауважують дослідники, у

політичній сфері ІТ виступають як специфічні комунікативні та управлінські матриці, що спроможні як оптимізувати державне управління, так і виступати інструментом впливу на електоральну поведінку громадян [59, с. 60].

Відповідно, сучасна концептуалізація ІТ охоплює не лише апаратне та програмне забезпечення, але й глобальні мережеві платформи, алгоритми штучного інтелекту, соціальні медіа та технології обробки великих даних (Big Data), які безпосередньо залучені до процесів політичного виробництва та ухвалення державних рішень.

Паралельно із цим суттєвих трансформацій зазнає і категорія «політичний процес», яка в класичній політології визначається як сукупність дій суб'єктів політики, спрямованих на завоювання, утримання та використання державної влади [5, с. 57].

У традиційній політичній теорії цей процес розглядався як ієрархічний, закритий та переважно інституціоналізований, де ключовими акторами виступали держава, політичні партії та легальні групи інтересів. В умовах мережевого суспільства політичний процес стає нелінійним, децентралізованим та багатовекторним [11, с. 15].

Сучасна політична динаміка розгортається у просторі, де старі інституційні логіки постійно переплітаються, конкурують або взаємодіють із новими мережевими логіками, такими як вірусні тренди у соціальних мережах, миттєва мобілізація громадян через месенджери чи низові цифрові рухи.

Таким чином, політичний процес у сучасному світі - це динамічна взаємодія між традиційними інституційними структурами та горизонтальними мережевими акторами щодо формування суспільного порядку денного.

Важливим внеском у розуміння взаємодії ІТ та політичного процесу є концепції «суспільства нагляду» та впливу алгоритмів на індивідуальну свободу. Алгоритми соціальних платформ, аналізуючи поведінкові дані користувачів, здатні штучно створювати персоналізовані інформаційні капсули («бульбашки фільтрів»), що неминуче призводить до радикалізації та поляризації політичного процесу [3, с. 45].

В українському науковому дискурсі на цьому аспекті наголошують дослідники, вказуючи, що віртуалізація політики створює ілюзію загальної партисипації (участі), тоді як реальні важелі впливу часто зміщуються до транснаціональних власників цифрових платформ або модераторів інформаційних потоків [8, с. 59].

Політичний процес, за таких умов, перетворюється на медіатизоване видовище, де ефективність політичного актора вимірюється не стільки його реальною програмою, скільки його цифровою присутністю та здатністю генерувати мережеву залученість аудиторії [6, с. 43].

Окрему увагу слід приділити зміні суб'єктного складу політичного процесу під впливом ІТ. Завдяки доступності та транскордонності інтернет-технологій, класична монополія держави на інформацію та формування смислів виявилася зруйнованою. Мережева інформаційна економіка дозволяє індивідам та автономним групам об'єднуватися для політичних дій без посередництва традиційних бюрократичних інституцій [15, с. 25]. Це породжує феномен мережевого активізму та е-демократії, де громадяни отримують інструменти прямого тиску на владні структури через електронні петиції, краудфандинг суспільних проєктів та онлайн-моніторинг державних витрат [22, с. 40].

Водночас, діалектика взаємовпливу ІТ та політичного процесу має амбівалентний характер. З одного боку, інформаційні технології виступають драйвером демократизації через інструменти електронного урядування [12, с. 53].

З іншого боку, цифровізація відкриває можливості для автократичних режимів у контексті цифрового нагляду, цензури та ведення гібридних інформаційних воєн [17, с. 30]. Політичний процес стає вразливим до кібератак на виборчу інфраструктуру та скоординованих кампаній із дезінформації, що здатні дестабілізувати систему національної безпеки [39, с. 56].

Таким чином, наукова концептуалізація «інформаційних технологій» та «політичного процесу» в межах цього дослідження базується на визнанні їхнього глибокого взаємопроникнення. Інформаційні технології розглядаються не як зовнішній технічний чинник, що впливає на політику ззовні, а як первинне структурне та комунікаційне середовище, всередині якого політичний процес набуває мережевого, гібридного, медіатизованого та високотехнологічного характеру, змінюючи традиційні параметри політичної участі, легітимації та функціонування державної влади.

Висновки до підрозділу 1.1

Аналіз теоретико-методологічних засад дослідження свідчить, що в умовах розбудови мережевого суспільства інформаційні технології та політичні процеси опинилися в стані глибокої взаємозалежності. Сучасні цифрові інструменти вже неможливо трактувати суто як технічні засоби для передачі чи обробки даних, оскільки вони перетворилися на один із ключових чинників трансформації всієї політичної системи. Саме через роботу цифрових комунікаційних мереж сьогодні формуються нові моделі громадянської залученості, змінюються формати ухвалення державних рішень, переформатовується логіка стосунків між владою і суспільством, а також модернізуються класичні політичні інститути.

Характерною рисою сучасного політичного процесу в межах мережевої архітектури стає його висока динамічність, децентралізація та багатовекторність. Традиційні суб'єкти політики тепер змушені ділити інформаційний та мобілізаційний простір із новими акторами - великими цифровими платформами, соціальними мережами, віртуальними спільнотами та лідерами думок, які здатні самотійно конструювати суспільний порядок денний. Така тенденція вказує на поступовий відхід від суворо ієрархічних моделей політичної взаємодії на користь гнучких мережеских форм організації суспільного життя.

Поряд із очевидними перевагами цифрових трансформацій, у роботі окреслено й суттєві ризики, що супроводжують цей процес. Серед них

особливу небезпеку становлять посилення непублічного інформаційного контролю, штучне закриття користувачів у межах «бульбашок фільтрів», стрімке поширення маніпуляцій та критична залежність суспільних настроїв від комерційних алгоритмів глобальних платформ. Як наслідок, хоча політична сфера й стає більш відкритою та партисипативною, вона одночасно набуває високої вразливості до зовнішніх інформаційних інтервенцій та прихованих технологічних впливів.

Таким чином, розгляд сутності інформаційних технологій у контексті політичного процесу дозволяє трактувати їх як взаємопов'язані складові нової суспільної реальності. Цифровізація є не просто зовнішнім чинником, що коригує політичне життя, а повноцінним середовищем його існування. Саме це середовище відтепер визначає специфіку політичної комунікації, механізми мобілізації громадян та особливості реалізації владних відносин у цифрову епоху.

1.2. Основні моделі та форми електронної демократії (e-Democracy)

Трансформація глобального політичного ландшафту під впливом четвертої промислової революції призвела до виникнення принципово нової архітектури публічного управління - електронної демократії. В сучасній політичній науці е-демократія інтерпретується не лише як сукупність дигітальних інструментів, а як комплексна стратегія реформування класичних інститутів народовладдя, що має на меті подолання кризи легітимності та політичної апатії громадян [12]. Основний концептуальний вектор розвитку цього феномену спрямований на децентралізацію влади, де технології стають не просто каналом передачі даних, а середовищем формування нового типу громадянської ідентичності.

Фундаментальним інституційним каркасом для розгортання цифрового народовладдя виступає система електронного урядування (e-Government). У науковому дискурсі важливо розмежовувати ці поняття: якщо e-Government

фокусується переважно на технологізації державних послуг та оптимізації адміністрування, то е-Democracy охоплює ширше коло процесів, включаючи волевиявлення, участь у дискусіях та контроль за владою [7]. В межах системного аналізу електронного урядування традиційно виокремлюють чотири ключові моделі взаємодії, кожна з яких має специфічний вплив на стабільність політичної системи.

Першою та найбільш видимою є модель G2C (Government-to-Citizen - уряд для громадян). Її сутність полягає у створенні «держави-сервісу», де взаємодія з інституціями максимально деперсоніфікована. Це дозволяє нівелювати людський фактор, що є критично важливим для країн із високим рівнем системної корупції. В українському контексті еволюція цієї моделі пройшла шлях від статичних урядових порталів до динамічної екосистеми «Дія». Аналіз цієї моделі в дипломній роботі дозволяє стверджувати, що цифровізація послуг сприяє формуванню «цифрової лояльності» виборця, коли ефективність влади оцінюється через зручність її онлайн-інструментів [21].

Модель G2B (Government-to-Business - уряд для бізнесу) відіграє роль стабілізатора економічних відносин у політичному процесі. Вона базується на принципах прозорості та відкритості даних (Open Data). Впровадження систем електронних закупівель та автоматизованої податкової звітності мінімізує можливості для олігархічного лобізму та тіньових домовленостей, що є необхідною умовою для демократичного розвитку держави [33]. Водночас внутрішні моделі G2G (Government-to-Government - уряд для уряду) та G2E (Government-to-Employee - уряд для службовців) забезпечують горизонтальну інтеграцію державних реєстрів. Без належної координації всередині державного апарату будь-які зовнішні цифрові ініціативи залишатимуться лише «фасадною демократією» [18, с. 45].

Теоретична верифікація е-демократії неможлива без критичного аналізу концепції публічної сфери, закладеної Юргеном Хабермасом. Трансформація

класичного «простору дебатів» у цифрову публічну сферу (Digital Public Sphere) радикально змінила природу політичної комунікації [48].

Якщо раніше доступ до публічного виступу був обмежений ресурсами та соціальним статусом, то мережеві технології створили ілюзію повної рівності учасників дискурсу. Проте сучасна політологічна думка дедалі частіше звертається до феномену «фрагментованої публічності». Дослідження демонструють, що замість раціонального діалогу в мережі виникають «інформаційні бульбашки» та «ехо-камери», які лише посилюють існуючі упередження виборців [9].

Алгоритмізація соціальних медіа призводить до того, що користувачі ізолюються від альтернативних точок зору, що руйнує фундамент демократичного консенсусу та провокує радикалізацію політичного життя.

Окрему увагу в структурі дипломної роботи варто приділити аналізу форм електронної участі (e-Participation), які диференціюються за ступенем залученості громадян у процес прийняття рішень. Найбільш дискусійною формою залишається електронне голосування (e-Voting). Попри успішні кейси (наприклад, досвід Естонії), глобальне впровадження дистанційного волевиявлення стримується високими ризиками кібервтручання та проблемою верифікації голосу при збереженні його анонімності [25].

Проте інструменти «м'якої участі», такі як електронні петиції, вже стали невід'ємною частиною української політичної реальності. Вони виконують функцію «клапана випуску пари» та дозволяють владі оперативно моніторити найбільш гострі суспільні запити, що сприяє запобіганню соціальним конфліктам [14].

Також перспективним напрямом є політичний краудсорсинг (Crowdlawmaking), де колективний інтелект спільноти залучається до спільної законотворчості, що підвищує якість та легітимність нормативних актів [30].

Завершальним етапом аналізу є розгляд проблеми «цифрового розриву» (Digital Divide). Це явище не є суто технічним, воно має глибоке соціально-

політичне коріння. Нерівність у доступі до технологій та рівні цифрової грамотності (Media Literacy) створює нові форми відчуження [41].

В умовах, коли участь у політичному житті дедалі більше залежить від володіння ІТ-інструментами, існує загроза формування «цифрової меритократії», де голоси вразливих груп населення (пенсіонерів, мешканців сільської місцевості) стають невидимими для політичної системи. Науковці підкреслюють, що без впровадження інклюзивної державної політики та програм подолання цифрової неписьменності, розвиток інформаційних технологій може призвести до ерозії демократичних цінностей, перетворюючи народовладдя на інструмент маніпулятивного впливу для найбільш технологічно розвинених груп [5].

Таким чином, розгляд моделей е-демократії свідчить про те, що успішна цифрова трансформація політичного процесу потребує не лише технічного оснащення, а й створення міцного правового каркасу, який би гарантував безпеку даних, захищав від маніпуляцій та забезпечував рівний доступ кожного громадянина до цифрового публічного простору.

Висновки до підрозділу 1.2

Аналіз базових моделей та практичних форм електронної демократії свідчить, що впровадження цифрових технологій суттєво розширює простір для громадянської залученості та виступає каталізатором модернізації класичних демократичних інститутів. Сьогодні цей феномен уже неможливо розглядати лише як перелік технічних новацій; він є цілісною архітектурою взаємодії між державою та суспільством, що покликана зробити політичні процеси більш відкритими, прозорими та інклюзивними.

По суті, розвиток цифрових інструментів став логічною відповіддю на системну кризу довіри до традиційних інститутів влади та суспільний запит на появу нових, більш оперативних механізмів впливу на державну політику.

Організаційним та технологічним фундаментом для таких трансформацій є система електронного урядування, яка оптимізує комунікацію на всіх рівнях - між державними структурами, громадянами,

бізнесом та самими управлінцями. Комплексна реалізація ключових моделей взаємодії (як-от взаємодія держави з громадянами, підприємницьким сектором, іншими органами влади чи державними службовцями) дозволяє докорінно змінити якість надання публічних послуг. Головним вектором цих змін стає побудова концепції «держави-сервісу», де завдяки цифровим інструментам доступ людини до адміністративних та управлінських процедур спрощується до кількох кліків, що мінімізує людський фактор і зміцнює суспільну довіру до інституцій.

Разом із тим, формування цифрової публічної сфери супроводжується появою специфічних загроз, які можуть нівелювати її позитивний потенціал. Штучне замикання користувачів у межах «інформаційних бульбашок», робота мережових «ехо-камер» та алгоритмічна сегрегація контенту суттєво знижують якість суспільної дискусії та провокують штучну поляризацію електорату. Це підтверджує тезу про те, що успішність електронної демократії визначається не стільки технічними параметрами платформ, скільки спроможністю самого суспільства зберігати різноманітність думок, вести конструктивний діалог та критично оцінювати споживану інформацію.

Важливе практичне значення в цьому контексті мають прикладні форми електронної участі, серед яких особливу динаміку демонструють інструменти онлайн-петицій, цифрові консультації з громадськістю та різноманітні краудсорсингові платформи. Їхня інтеграція в політичне життя не лише стимулює громадянську активність, а й змушує владу зважати на реальні суспільні інтереси під час ухвалення рішень.

Водночас реальні перспективи цих інструментів прямо залежать від вирішення соціально-технологічних проблем: подолання цифрового розриву між різними верствами населення, системного підвищення медіаграмотності та забезпечення рівного доступу кожного громадянина до мережевої інфраструктури.

У підсумку можна стверджувати, що електронна демократія є стратегічним вектором еволюції сучасних політичних систем, який органічно

поєднує інноваційні технологічні рішення з базовими принципами суспільної підзвітності влади. Проте її повноцінне та безпечне функціонування можливе лише за умови створення комплексної правової, організаційної та соціальної бази, яка гарантуватиме справедливе, захищене та інклюзивне використання цифрових інструментів у публічній сфері.

1.3. Вплив Big Data та штучного інтелекту (AI) на суб'єктів політики

У сучасному політичному дискурсі дедалі виразніше постає проблема фундаментальної трансформації суб'єктності під тиском технологічного прогресу. Використання великих даних (Big Data) та систем штучного інтелекту (ШІ) перестало бути виключно технічним питанням оптимізації виборчих штабів, перетворившись на стратегічний чинник переформатування політичного простору. Наукове осмислення цього процесу потребує аналізу того, як алгоритмічні системи впливають на когнітивні механізми прийняття рішень та як змінюється ієрархія владних відносин у цифрову епоху [11].

Ключовим суб'єктом, що зазнає трансформації, є політичні партії та лідери, чия діяльність усе більше підпорядковується логіці предиктивної аналітики. Використання Big Data дозволяє акумулювати колосальні масиви інформації про користувацьку активність, геолокацію, споживчі кошики та навіть емоційні реакції виборців у соціальних мережах. Це породжує феномен «алгоритмічного маніпулювання», де суб'єкт політики оперує не ідеологічними доктринами, а динамічними психографічними профілями аудиторії [26].

Завдяки мікротаргетингу стає можливим сегментувати електоральне поле на мікрогрупи, пропонуючи кожній із них специфічну візію реальності, що часто призводить до деградації загальнонаціонального політичного порядку денного та фрагментації суспільної свідомості.

Окрему увагу слід приділити ролі штучного інтелекту як автономного або напівавтономного суб'єкта політичної комунікації. Розгортання масштабних бот-мереж, керованих інтелектуальними алгоритмами, дозволяє здійснювати когнітивний тиск на опонентів та штучно конструювати «спіралі мовчання». Технологія «астротурфінгу», що імітує низову громадську підтримку, створює у виборця хибне уявлення про мейнстрімні настрої, що суттєво впливає на результати волевиявлення [34].

Крім того, виникнення генеративних моделей ШІ, здатних створювати гіперреалістичні дипфейки, ставить під загрозу інститут політичної репутації. Суб'єкт політики в таких умовах стає надзвичайно вразливим до інформаційних операцій, де межа між реальним фактом та згенерованою симуляцією остаточно розмивається [42].

Державні інституції як суб'єкти управління також проходять етап реконфігурації під впливом «data-driven» підходу. Впровадження інтелектуальних систем у процеси публічного адміністрування дозволяє автоматизувати аналіз соціальних ризиків та прогнозувати динаміку протестних настроїв. Проте така інтелектуалізація управління несе в собі ризик виникнення «алгоритмічного детермінізму», коли складні соціальні проблеми зводяться до математичних моделей, що ігнорують гуманістичний аспект політики [19].

Для правлячих еліт виникає небезпечна спокуса використання ШІ для превентивного соціального інжинірингу, що в країнах із перехідною демократією може трансформуватися у форми цифрового авторитаризму, де контроль здійснюється не через прямий примус, а через невидимі алгоритмічні обмеження [50].

У контексті трансформації суб'єктності неможливо оминути роль великих технологічних корпорацій (Big Tech), які фактично перетворюються на нових глобальних політичних акторів. Володіючи монополією на дані та алгоритми ранжування інформації, ці суб'єкти отримують можливість негласно впливати на формування політичних пріоритетів цілих націй.

Владний ресурс сьогодні переміщується від офіційних державних інституцій до власників когнітивних платформ, що породжує проблему демократичного контролю над приватними алгоритмами, які визначають, що саме бачить і чує виборець [15, с. 38].

Для пересічного громадянина як суб'єкта політики наслідки впровадження Big Data та ШІ є найбільш суперечливими. З одного боку, індивід отримує інструменти для миттєвого доступу до політичної інформації та самоорганізації. З іншого - він стає об'єктом безперервного алгоритмічного спостереження. «Цифровий слід» громадянина стає ресурсом для маніпуляцій, а постійне перебування в «інформаційних коконах» знижує здатність до критичної оцінки альтернативних точок зору [22].

Таким чином, політична суб'єктність індивіда в цифрову епоху опиняється під загрозою, оскільки вибір часто робиться під впливом ретельно прорахованих алгоритмічних підказок, які експлуатують ірраціональні аспекти людської психіки.

Підсумовуючи, можна констатувати, що Big Data та штучний інтелект не просто доповнюють існуючі політичні технології, а створюють нову онтологію політичного процесу. Суб'єкти політики змушені адаптуватися до умов, де швидкість обробки даних та точність алгоритмічного прогнозу стають важливішими за традиційні методи політичної боротьби. Головним викликом сучасності є необхідність розробки нових етичних та правових стандартів, які б гарантували збереження людської гідності та автономії в умовах тотальної алгоритмізації політичного життя.

Висновки до підрозділу 1.3

Дослідження впливу технологій Big Data та інструментів штучного інтелекту на сучасних політичних суб'єктів свідчить, що ці цифрові інновації виступили потужним каталізатором глибоких якісних змін. Збір і обробка колосальних масивів інформації, а також упровадження алгоритмічних систем докорінно переформатували логіку вибудовування політичних стратегій, трансформували канали комунікації з електоратом і змінили підходи до

ухвалення управлінських рішень. Сучасна політична діяльність усе сильніше спирається на глибинну аналітику даних, моделювання суспільних настроїв та інструменти точкового впливу, що дозволяє значно підвищити результативність виборчих кампаній і розширити тактичні можливості кандидатів чи партій.

Практика застосування Big Data відкриває перед політичними силами унікальні можливості для детального моделювання поведінкових моделей громадян, інтересів та прихованих уподобань громадян. Завдяки цьому політичний діалог стає максимально адресним: технології мікротаргетингу дають змогу створювати унікальні інформаційні меседжі для кожної окремої соціальної мікрогрупи. Зворотним боком такої персоналізації є серйозна загроза прихованого маніпулювання громадською думкою. Коли політичний вплив переноситься з площини відкритих публічних дискусій у простір закритих алгоритмічних маніпуляцій, це суттєво деформує класичні принципи чесної політичної конкуренції.

Паралельно з цим штучний інтелект перетворюється на базовий елемент як повсякденної політичної комунікації, так і запеклого інформаційного протиборства. Поширення автоматизованих систем, бот-мереж, генеративних текстових моделей та високореалістичних дипфейків майже повністю стирає межу між правдивим контентом і професійно сфабрикованою дезінформацією. Такий стан справ кидає серйозний виклик прозорості виборчих процесів, підриває залишки суспільної довіри до демократичних інституцій та загрожує загальній інформаційній безпеці країни. Це актуалізує нагальну потребу у створенні дієвих правових та технічних бар'єрів для контролю за використанням ШІ в публічній політиці.

Не менш важливим наслідком цифровізації є трансформація ролі самих державних інститутів та поява нових впливових акторів. З одного боку, алгоритми штучного інтелекту відкривають привабливі перспективи для оптимізації державного менеджменту, автоматизації рутинних процедур та прогнозування соціально-політичних ризиків. З іншого - надмірне захоплення

алгоритмічними рішеннями несе в собі загрози формування цифрового авторитаризму, де тотальний контроль над даними звужує простір для громадянських свобод. Більше того, у сучасному світі особливу політичну вагу здобувають глобальні технологічні корпорації. Володіючи монопольним контролем над цифровими платформами та інформаційними потоками, вони отримують реальні важелі впливу на формування світових трендів і суспільного порядку денного.

У підсумку можна стверджувати, що Big Data та штучний інтелект кардинально змінюють архітектуру сучасної політики, приносячи із собою як інноваційні інструменти розвитку, так і серйозні системні виклики. Продуктивна інтеграція цих технологій у політичне життя можлива лише за умови створення гнучкої нормативної бази, жорсткого дотримання етичних стандартів, прозорості самих алгоритмів та безумовного захисту персональних даних. Тільки за такого збалансованого підходу цифрові інновації працюватимуть на підвищення ефективності управління, не руйнуючи при цьому фундаментальних демократичних цінностей та свободи вибору кожної людини.

Висновки до розділу I

У першому розділі кваліфікаційної роботи було здійснено всебічний теоретико-методологічний аналіз особливостей та характеру впливу інформаційних технологій на сучасні політичні процеси.

Масштабне теоретичне підґрунтя дозволило чітко окреслити, що стрімке поширення цифрових інструментів не просто коригує окремі елементи політичного життя, а фундаментально переформатовує базові механізми функціонування всієї політичної системи.

Цифровізація суттєво змінює класичні канони політичної комунікації, диктує нові правила інформаційного обміну та закладає абсолютно інші координати для взаємодії між державними інститутами, інститутами громадянського суспільства та безпосередньо громадянами.

Детальний аналіз архітектури мережевого суспільства переконує, що інформаційні технології повністю переросли рамки суто допоміжного або технічного інструментарію. Сьогодні вони виступають повноцінним та невід'ємним структурним елементом сучасного політичного середовища.

Самі політичні процеси під цим впливом набувають чітких ознак розсосередженості, високої динамічності та інтерактивності, де мережеві комунікації перетворюються на головне рушійне джерело для конструювання суспільної думки, швидкої мобілізації громадян та реалізації електоральних практик.

Проте цей процес супроводжується серйозними системними викликами. Глобальна цифровізація принесла із собою критичні загрози для національної та інформаційної безпеки, створила передумови для масштабного прихованого маніпулювання масовою свідомістю, а також сформувала небезпечну залежність суспільних настроїв від алгоритмів приватних цифрових платформ.

Вивчення еволюції моделей та прикладних форм електронної демократії підтверджує, що новітні технології відкривають перед суспільством реальні канали для безпосереднього залучення людей до процесів ухвалення важливих державних рішень.

Послідовне впровадження інструментів електронного урядування, різноманітних платформ для цифрової участі та прямих каналів онлайн-комунікації робить діяльність органів публічної влади значно прозорішою, стимулює низову громадянську активність та модернізує традиційні демократичні процедури відповідно до вимог часу.

Разом із тим, реальна життєздатність та ефективність таких інструментів не є автоматичною. Вона прямо корелює з рівнем базової медіаграмотності суспільства, наявністю чіткої та гнучкої правової бази, а також спроможністю держави подолати цифровий розрив і забезпечити рівний доступ до мережевої інфраструктури для всіх соціальних груп.

Окремим вагомим фактором трансформації сучасної політичної архітектури виступає активне залучення технологій Big Data та систем штучного інтелекту, які кардинально змінюють принципи діяльності ключових суб'єктів політики.

Робота з великими масивами даних та складними алгоритмічними моделями дозволяє значно підвищити точність політичного прогнозування, оптимізувати стратегії виборчих кампаній та вивести на якісно новий рівень процеси державного менеджменту.

Утім, зворотний бік використання цих технологій актуалізує низку гострих етичних, правових та безпекових дилем.

Особливу стурбованість викликають ризики непублічного маніпулювання електоральною поведінкою, використання персональних даних громадян без їхнього реального контролю, а також безпрецедентне зростання політичної ваги глобальних технологічних корпорацій, які через контроль над інформаційними потоками отримують реальні важелі впливу на світовий порядок денний.

Підсумовуючи викладене, можна стверджувати, що інформаційні технології остаточно утвердилися як невід'ємна складова сучасної політичної реальності, яка визначає магістральні напрями її подальшого розвитку.

Їхній трансформаційний вплив має наскрізний характер і охоплює абсолютно всі рівні політичної архітектури - від індивідуальних проявів громадянської активності до внутрішньої діяльності державних інститутів та глобальних міжнародних процесів.

Саме тому глибоке та системне вивчення прикладних механізмів функціонування цифрових технологій у публічній сфері залишається одним із найбільш пріоритетних напрямів для сучасних політичних досліджень і виступає обов'язковою умовою для забезпечення стабільного та захищеного демократичного розвитку суспільства.

РОЗДІЛ 2 АНАЛІЗ ТРАНСФОРМАЦІЇ КЛЮЧОВИХ ПОЛІТИЧНИХ ІНСТИТУТІВ ТА ЯВИЩ

2.1. Зміни у політичній комунікації та виборчих кампаніях

Сучасна еволюція політичної комунікації в межах виборчих процесів характеризується фундаментальним переходом від стратегій масового впливу до високосегментованих технологій мікротаргетингу. У цифрову епоху виборча кампанія перестає бути статичним набором лозунгів, трансформуючись у динамічну, інтерактивну систему, де ключовим ресурсом стає не лише ефірний час на центральних телеканалах, а контроль над потоками даних та алгоритмами їх дистрибуції.

Ця трансформація зумовила виникнення нової комунікативної реальності, у якій традиційні медіа-ефекти поступаються місцем мережевим ефектам, а політичний дискурс стає дедалі більш фрагментованим та емоційно насиченим [4].

Однією з найбільш радикальних змін є трансформація темпоральності виборчого процесу. Концепція «постійної виборчої кампанії» (permanent campaign) набула в мережевому середовищі абсолютного значення. Якщо раніше політична активність мала яскраво виражені піки під час агітаційного періоду, то сьогодні суб'єкти політики змушені підтримувати високий рівень присутності в інформаційному полі безперервно.

Будь-яка пауза в цифровій активності сприймається аудиторією як втрата актуальності, що змушує політичних акторів постійно генерувати інфоприводи, часто жертвуючи якістю та змістовністю контенту заради його віральності. У такому контексті політична комунікація зміщується в бік «політики реального часу», де швидкість реакції на подію стає важливішою за стратегічну виваженість позиції [10].

Важливим вектором трансформації є зміна архітектури взаємовідносин «кандидат - виборець». Цифрові платформи дозволили подолати ієрархічний

бар'єр, створивши ілюзію прямої, горизонтальної комунікації. Політик у соціальних мережах змушений конструювати образ «близької людини», використовуючи неформальну мову, стрімлінги з особистого простору та інтерактивні опитування.

Це явище, відоме як «персоналізація політики», призводить до того, що емоційна прив'язаність до лідера та його цифрової персони домінує над раціональним оцінюванням партійної програми. Виборець у такій системі перестає бути лише пасивним об'єктом впливу, перетворюючись на активного ретранслятора політичного контенту.

Через механізми репостів, коментування та створення власного креативу прихильники стають добровільними учасниками виборчих штабів, що забезпечує органічне охоплення аудиторії, недоступне для традиційної реклами [23].

Проте горизонтальність мережевої комунікації є багато в чому маніпулятивною конструкцією, оскільки за нею стоять складні математичні моделі. Використання великих даних дозволяє виборчим штабам створювати психографічні портрети електорату з неймовірною точністю. Замість єдиного повідомлення для всієї країни, кандидати поширюють тисячі варіацій одного й того самого меседжу, адаптованого під конкретні страхи чи сподівання окремих груп.

Це породжує серйозний демократичний виклик: виборці в одній країні можуть бачити абсолютно різні «реальності» виборчих кампаній, що унеможлиблює загальнонаціональний консенсус і сприяє поляризації суспільства. Політичний дискурс замикається в межах «ехо-камер», де алгоритми платформ підкріплюють існуючі переконання користувачів, обмежуючи їхній доступ до альтернативних точок зору [31].

Окремо слід виділити трансформацію інструментарію негативної комунікації та «чорних» технологій. У сучасних кампаніях пряма антиреклама поступається місцем складним операціям впливу, таким як використання бот-мереж для створення ефекту «штучної більшості» або дискредитація опонента

через розповсюдження дезінформації в месенджерах, де контроль за контентом є мінімальним. Телеграм-канали в українському сегменті стали яскравим прикладом анонімізованої політичної комунікації, де відсутність редакційної політики дозволяє поєднувати інсайди з маніпулятивними вкидами, миттєво змінюючи електоральні настрої.

В умовах такої інформаційної асиметрії виборець часто втрачає здатність верифікувати джерела, що робить когнітивну стійкість критичним фактором безпеки політичного процесу [15, с. 47].

Таким чином, зміни у політичній комунікації та виборчих кампаніях відображають глибинний перехід від демократії переконання до демократії алгоритмів. Сучасна виборча інженерія дедалі більше покладається на технологічні переваги в обробці даних та маніпулятивні можливості цифрових платформ.

Це вимагає від суспільства не лише підвищення рівня медіаграмотності, а й розробки нових правових механізмів регулювання цифрової агітації, які б гарантували прозорість алгоритмів та захищали б волевиявлення громадян від прихованих технологічних впливів.

Висновки до підрозділу 2.1

Аналіз новітніх тенденцій трансформації електоральних процесів, представлений у цьому підрозділі, дозволяє сформулювати кілька важливих висновків щодо того, як саме змінюється сучасна політична комунікація.

Сьогодні відбувається поступовий відхід від звичних методів масового впливу через традиційні ЗМІ до складних технологій мікротаргетингу.

У цифрову епоху виборча кампанія перестає бути просто набором статичних лозунгів на білбордах чи телебаченні, вона перетворюється на динамічну систему, де головним ресурсом стає контроль за потоками даних та алгоритмами їхнього розповсюдження.

Традиційні медіа-ефекти сьогодні замінюються мережевими, що робить політичний дискурс більш фрагментованим та емоційним.

Одним із найбільш відчутних наслідків цієї трансформації є зміна динаміки та часових меж виборчого процесу.

Концепція постійної виборчої кампанії в інтернет-середовищі стала абсолютною реальністю. Якщо раніше політики активізувалися переважно під час офіційного агітаційного періоду, то зараз вони змушені підтримувати свою присутність в інформаційному полі безперервно.

Будь-яка пауза в соціальних мережах одразу сприймається аудиторією як втрата актуальності чи слабкість позицій. Це змушує штаби постійно генерувати нові інфоприводи, через що якість та змістовність контенту часто приносяться в жертву його віральності та здатності швидко збирати охоплення. У таких умовах швидкість реакції на подію стає набагато важливішою за стратегічно виважену та аргументовану позицію.

Не менш важливою є й перебудова взаємин між кандидатом та виборцем. Цифрові платформи частково зруйнували колишні ієрархічні бар'єри, створивши для користувачів ілюзію прямого, горизонтального спілкування.

Політик у соцмережах тепер змушений конструювати образ максимально близької людини, використовуючи неформальний стиль, прямі ефіри з особистого простору та інтерактивні опитування.

Така прискорена персоналізація політики призводить до того, що емоційна прив'язаність до лідера та його цифрового іміджу починає домінувати над раціональним аналізом партійної програми.

При цьому сам виборець перестає бути просто пасивним об'єктом агітації. Через механізми репостів, коментарів та створення власного контенту прихильники фактично перетворюються на добровільних учасників виборчих штабів, допомагаючи поширювати потрібні меседжі безкоштовно та органічно.

Проте варто розуміти, що вся ця нібито доступна горизонтальність мережевої комунікації є маніпулятивною за своєю природою, адже за нею стоять складні математичні алгоритми. Збір великих даних дозволяє виборчим

штабам створювати точні психографічні портрети електорату. Замість одного універсального звернення до всієї країни кандидати тепер транслують тисячі дрібних варіацій одного й того самого меседжу, адаптуючи його під конкретні страхи чи очікування окремих вузьких груп.

Це створює серйозний виклик для демократії: виборці в межах однієї держави починають бачити абсолютно різні реальності виборчих кампаній, що руйнує простір для суспільного діалогу та підсилює поляризацію. Політичний дискурс замикається в межах ехо-камер, де алгоритми лише підкріплюють уже наявні переконання користувачів і повністю обмежують їхній доступ до альтернативних точок зору.

Окрему небезпеку становить еволюція інструментів негативної комунікації та «чорних» технологій. Традиційна антиреклама сьогодні поступається місцем складним операціям впливу, таким як використання мереж ботів для створення ефекту штучної більшості або дискредитація опонентів через анонімні канали.

Для українського політичного сегменту яскравим прикладом такої анонімізованої комунікації стали Telegram-канали. Відсутність чіткої редакційної політики та контролю за контентом дозволяє там легко поєднувати реальні інсайди з відвертими маніпулятивними вкидами, оперативно впливаючи на електоральні настрої. В умовах такої інформаційної асиметрії звичайний виборець часто втрачає здатність перевіряти джерела, тому когнітивна стійкість та медіагігієна стають критично важливими факторами безпеки.

Підсумовуючи, можна сказати, що всі ці зміни свідчать про поступовий перехід від демократії переконання до демократії алгоритмів. Сучасний виборчий процес дедалі сильніше покладається на технологічні переваги в обробці даних та маніпулятивні можливості великих платформ. Це вимагає від суспільства не лише підвищення рівня особистої медіаграмотності, а й розробки нових правових механізмів регулювання цифрової агітації, які б

могли гарантувати прозорість роботи алгоритмів і захистили волевиявлення громадян від прихованих технологічних впливів.

2.2. IT як інструмент державного управління та підвищення прозорості

Трансформація державного управління під впливом інформаційних технологій у сучасних політичних реаліях перестала бути лише питанням технічної модернізації канцелярій, перетворившись на стратегічний напрям реформування самої сутності публічної влади. Впровадження IT-інструментів у систему державного адміністрування спрямоване на вирішення фундаментального протиріччя між закритою бюрократичною ієрархією та вимогою суспільства щодо відкритості, підзвітності та ефективності політичних інститутів.

У цьому контексті цифровізація виступає не просто як медіатор, а як системний архітектор нової моделі управління - «цифрового левіафана», де контроль здійснюється через прозорість алгоритмів та автоматизацію управлінських процесів [19].

Центральним елементом використання IT для підвищення прозорості є перехід до концепції «держави як платформи» (Government as a Platform). Ця парадигма передбачає створення єдиного цифрового контуру, у якому взаємодія між різними гілками влади, бізнесом та громадянами відбувається в режимі реального часу без посередництва чиновника. Впровадження систем електронного документообігу та інтегрованих державних реєстрів дозволяє мінімізувати суб'єктивізм у прийнятті рішень. Коли управлінський цикл стає цифровим, кожен етап проходження документа або розподілу ресурсу залишає «цифровий слід», який може бути верифікований незалежними аудитором або громадськістю.

Для більш детального розуміння глибини трансформаційних процесів у системі публічного адміністрування, доцільно здійснити порівняльний аналіз

ключових характеристик традиційної бюрократичної та новітньої цифрової моделей управління (див. табл. 2.1).

Таблиця 2.1. Порівняльна характеристика традиційної та цифрової моделей державного управління

Критерій порівняння	Традиційна (бюрократична) модель	Цифрова (сервісна) модель (e-Government)
Принцип взаємодії	Вертикальна ієрархія, наявність посередника (чиновника).	Мережева структура, пряма взаємодія через платформи.
Рівень прозорості	Закритість процесів, доступ до інформації за запитом.	«Прозорість за замовчуванням», відкриті дані (Open Data).
Швидкість процесів	Тривалий паперовий документообіг, часові затримки.	Обробка даних у режимі реального часу (Real-time).
Суб'єктивність	Високий вплив людського фактора (ризик корупції).	Автоматизація та алгоритмізація прийняття рішень.
Зворотний зв'язок	Опосередкований, формальний та повільний.	Миттєвий, через системи онлайн-моніторингу та оцінки.
Доступність послуг	Територіальна прив'язка до кабінетів та графіків роботи.	Принцип 24/7, доступність з будь-якої точки світу.

Дані таблиці 2.1 підтверджують, що впровадження ІТ-інструментів не просто прискорює існуючі процедури, а докорінно змінює філософію управління, де пріоритетом стає не контроль, а якість та прозорість надання державних послуг [45].

Це створює умови для реалізації принципу «прозорості за замовчуванням» (transparency by design), де приховування інформації стає технологічно складнішим і дорожчим процесом, ніж її оприлюднення.

Одним із найпотужніших інструментів боротьби з корупцією та підвищення ефективності державного сектора є цифровізація публічних фінансів та закупівель. Прикладом успішної імплементації ІТ у цій сфері є українська система ProZorro та портал Spending.gov.ua. Використання великих даних (Big Data) для моніторингу тендерних процедур дозволяє виявляти аномалії та потенційні змови на ранніх етапах, ще до моменту підписання контракту.

Математичні алгоритми здатні аналізувати зв'язки між учасниками торгів, виявляти афілійованість осіб та порівнювати ціни з ринковими показниками в автоматичному режимі.

Це радикально змінює роль контролюючих органів: від реактивного реагування на вчинені правопорушення вони переходять до превентивного моніторингу ризиків, що суттєво підвищує рівень довіри інвесторів та міжнародних партнерів до політичного керівництва держави [33].

Іншим критично важливим вектором є розвиток Open Data (відкритих даних) як інструменту громадського контролю. Публікація наборів даних про діяльність органів влади у машиночитаних форматах дозволяє активістам, журналістам та науковцям створювати аналітичні сервіси для відстеження ефективності державної політики.

Відкритість реєстрів нерухомості, декларацій державних службовців та екологічного моніторингу перетворює кожного громадянина на потенційного суб'єкта контролю. Це стимулює формування «культури підзвітності», де державний службовець усвідомлює невідворотність публічного розголосу у разі зловживання владою. Таким чином, ІТ створюють горизонтальну систему стримувань і противаг, яка доповнює традиційний розподіл влади [7, с. 50].

Проте підвищення прозорості через ІТ має і зворотний бік, який потребує глибокого аналізу. Існує ризик виникнення «фасадної прозорості», коли органи влади публікують величезні масиви нерелевантної або фрагментованої інформації, що створює ілюзію відкритості при збереженні закритих вузлів прийняття стратегічних рішень. Крім того, автоматизація

державного управління породжує проблему алгоритмічної відповідальності. Якщо рішення про надання соціальної допомоги або нарахування штрафу приймається автоматизованою системою (ШІ), виникає питання: хто несе політичну та юридичну відповідальність у разі помилки алгоритму? Відсутність прозорості самих кодів і логіки роботи державних ШІ-систем може призвести до нової форми технократичного авторитаризму, де бюрократія ховається за «неупередженістю» програмного забезпечення [15, с. 38].

Важливим аспектом є також використання ІТ для моніторингу якості надання публічних послуг. Впровадження систем зворотного зв'язку, електронних черг та оцінки сервісу громадянами в режимі реального часу створює конкурентне середовище всередині державного апарату. Це стимулює перехід від каральної моделі управління до сервісної. Громадянин починає сприймати державу не як ворожий апарат примусу, а як ефективного провайдера послуг, що є запорукою політичної стабільності та соціальної згуртованості. В умовах кризових ситуацій, таких як пандемії або військові конфлікти, здатність держави швидко перевести управлінські процеси в цифровий формат стає питанням національної безпеки та виживання політичної системи [21].

Інформаційні технології є не просто інструментарієм, а фундаментом для побудови нової якості державного управління. Вони забезпечують перехід від «аналогової» закритості до «цифрової» прозорості, де ефективність вимірюється не кількістю звітів, а реальним впливом на добробут громадян та рівнем їхньої довіри до інституцій. Однак успішна трансформація можлива лише за умови паралельного розвитку правового регулювання, яке б гарантувало безпеку даних та запобігало використанню цифровізації як інструменту тотального спостереження.

Висновки до підрозділу 2.2.

Дослідження того, як інформаційні технології впливають на публічне адміністрування, дозволяє зробити висновок, що цифровізація повністю змінює саму логіку взаємодії між державою та громадянами. Якщо порівняти традиційну та сучасну моделі, то стає очевидним масштабний перехід від закритих, вертикальних бюрократичних структур до прозорих мережеских платформ.

Коли впроваджується концепція «держави як платформи» і починає діяти принцип «прозорості за замовчуванням», роль людського фактора мінімізується, а більшість управлінських процесів автоматизується. Це не просто дозволяє отримувати послуги в режимі 24/7, а й створює чіткий «цифровий слід», який сильно ускладнює звичні корупційні схеми. Хорошим прикладом тут є успішна робота наших систем ProZorro та Spending.gov.ua.

Ще одним важливим результатом цієї трансформації є поява нових інструментів для громадського контролю завдяки розвитку Open Data. Оскільки державні реєстри стають відкритими, а дані публікуються у зручних машиночитаних форматах, активна частина суспільства отримує реальну можливість моніторити дії влади.

Це поступово формує нормальну культуру підзвітності серед держслужбовців. Проте в цьому процесі є й серйозні ризики. Наприклад, загроза так званої «фасадної прозорості», коли органи влади викидають у публічний простір величезні масиви другорядної інформації, щоб створити ілюзію відкритості, але при цьому ховають реальні центри прийняття рішень.

Крім того, автоматизація управління та залучення штучного інтелекту піднімають складне питання: хто саме має нести юридичну відповідальність у разі помилки алгоритму? Якщо логіка роботи таких програм залишатиметься закритою, є ризик отримати нову форму технократичного авторитаризму.

Інформаційні технології допомагають державі еволюціонувати від звичного карального апарату примусу до зручного сервісного провайдера. Це критично важливо для стабільності та витривалості всієї системи, особливо в умовах нинішніх криз та безпекових викликів. Проте, щоб така модель

функціонувала ефективно, потрібне якісне правове регулювання. Держава має забезпечити повну прозорість робочих алгоритмів, надійно захистити персональні дані людей і зробити все, щоб корисні цифрові сервіси не перетворилися на інструменти прихованого контролю та тотального спостереження за суспільством.

2.3. Новітні виклики: дезінформація, «ехо-камери» та кіберзагрози

Еволюція інформаційних технологій, поряд із розширенням демократичних свобод, сформувала принципово нове поле ризиків, що загрожують стабільності політичних систем та національній безпеці держав.

Сучасні виклики цифрової епохи - дезінформація, феномен «ехо-камер» та кіберзагрози - мають не лише технічний чи інформаційний характер, а є інструментами системного впливу на когнітивну сферу суспільства. Вони спрямовані на дестrukцію ціннісних орієнтирів, підриг довіри до державних інституцій та маніпулювання виборчими процесами, що робить їх аналіз критично важливим для розуміння трансформації сучасного політичного процесу [15].

Дезінформація та стратегії «постправди». У сучасному цифровому просторі дезінформація трансформувалася у високотехнологічну зброю когнітивної війни. На відміну від класичної пропаганди минулого століття, сучасні маніпулятивні стратегії базуються на використанні штучного інтелекту та алгоритмів віральності.

Це дозволяє поширювати контент зі швидкістю, яка в геометричній прогресії перевищує можливості офіційного спростування. Феномен «постправди» полягає в тому, що емоційне забарвлення новини та її відповідність існуючим упередженням аудиторії стають важливішими за її фактичну достовірність.

Найбільш небезпечним проявом цього є технологія «дипфейків» (deepfakes). Використання генеративно-змагальних мереж (GAN) дозволяє

створювати відеоматеріали, де політичні лідери «проголошують» заяви, яких ніколи не робили.

Прикладом із реального життя є спроба розповсюдження фальсифікованого відеозвернення Президента України про капітуляцію в березні 2022 року. Хоча цей конкретний кейс був швидко викритий, він продемонстрував потенціал технології для миттєвої дестабілізації лінії фронту та суспільного порядку.

В умовах виборчих кампаній такі технології можуть використовуватися для «вкидів» у «день тиші», коли законні механізми спростування вже не встигають подіяти на волевиявлення [34].

Алгоритмічна поляризація та «ехо-камери». Феномен «ехо-камер» (echo chambers) та «інформаційних бульбашок» (filter bubbles) є прямим наслідком комерційної логіки соціальних платформ. Алгоритми рекомендацій налаштовані на максимізацію часу перебування користувача в мережі. Для цього система пропонує контент, який викликає сильний емоційний відгук і підтверджує вже сформовану картину світу людини. Як наслідок, користувач опиняється в ізольованому інформаційному просторі, де альтернативні погляди або блокуються, або подаються в негативному контексті.

Це призводить до радикалізації політичних настроїв, оскільки в межах «ехо-камери» будь-яка поміркована позиція витісняється більш радикальною. У житті ми спостерігаємо це на прикладі політичної ситуації в США (2020–2024 рр.), де прихильники різних політичних таборів існують у діаметрально протилежних інформаційних реальностях. Таке розділення унеможливлює раціональний політичний діалог, перетворюючи опонентів на «ворогів», що підриває фундамент демократичного консенсусу та веде до загрози соціальних конфліктів [9].

Кіберзагрози як інструмент політичної дестабілізації. Кібератаки у політичному вимірі еволюціонували від простого вандалізму до складних операцій із втручання в критичну інфраструктуру та виборчі системи. Характерною рисою сучасних кіберзагроз є їхня анонімність та

транскордонність, що дозволяє авторитарним режимам приховано впливати на політичні процеси в демократичних країнах. Для систематизації цих ризиків доцільно розглянути порівняльну таблицю.(див. табл. 2.2)

Таблиця 2.2. Класифікація цифрових викликів та їх політичних наслідків

Тип виклику	Технологічний механізм	Політичний наслідок	Приклад / Кейс
Когнітивна дезінформація	Дипфейки, ШІ-боти, мікротаргетинг.	Руйнація віри в істину, хаотизація виборів.	Спроби зриву мобілізації в Україні через Telegram.
Алгоритмічні «ехо-камери»	Персоналізовані стрічки рекомендацій.	Соціальна атомізація, неможливість консенсусу.	Поляризація навколо питань вакцинації або Brexit.
Кібершпигунство та Hacktivism	Фішинг, взлом хмарних сховищ.	Оприлюднення компромату, шантаж еліт.	Взлом пошти штабу Е. Макрона або Г. Клінтон.
Інфраструктурні атаки	DDoS, віруси-шифрувальники.	Параліч державного апарату, паніка.	Атака на «Київстар» та сервіси Дія (2023-2024).

Дані таблиці 2.2 демонструють, що цифрові загрози діють за принципом синергії: кібератака супроводжується дезінформаційною кампанією, яка максимально ефективно розповсюджується через «ехо-камери» радикалізованих груп.

В Україні ці виклики мають екзистенційний характер. Масштабна атака на оператора зв’язку «Київстар» у грудні 2023 року була яскравим прикладом того, як технічна вразливість перетворюється на політичний чинник, викликаючи відчуття незахищеності та паніку [42].

Механізми протидії та стратегії цифрової стійкості. Дослідження новітніх викликів було б неповним без аналізу стратегій цифрової

резистентності (digital resilience). Важливим аспектом є те, що сучасні загрози експлуатують не лише технічні, а й психологічні вразливості людського сприйняття.

У цьому контексті виникає необхідність впровадження концепції «когнітивної безпеки», яка передбачає захист свідомості виборця від деструктивних алгоритмічних впливів.

Одним із інструментів є механізм fact-checking, проте сьогодні держава має переходити до технології «пребункінгу» (prebunking) - превентивного навчання громадян методам маніпуляції. Ключові напрями захисту систематизовано у таблиці 2.3.

Таблиця 2.3. Стратегічні напрями мінімізації цифрових ризиків у політичному процесі

Напрямок стратегії	Інструменти реалізації	Очікуваний результат
Нормативно-правовий	Законодавче регулювання соцмереж; маркування ШП.	Юридична відповідальність за дезінформацію.
Технологічний	Суверенний кіберзахист; аудит алгоритмів.	Технічна стійкість критичної інфраструктури.
Освітньо-соціальний	Програми з медіаграмотності; гігієна даних.	Формування критичного мислення у виборців.
Міжнародний	Створення кібер-альянсів; спільні санкції.	Глобальна ізоляція джерел кіберагресії.

Підсумовуючи, можна стверджувати, що виклики цифрової епохи не мають суто технічного вирішення. Політична стабільність у майбутньому залежатиме від здатності держави збалансувати технологічний прогрес із захистом демократичних цінностей. Дезінформація та кіберзагрози виступають не лише як перешкоди, а й як каталізатори модернізації демократичних інститутів, змушуючи їх ставати більш адаптивними та прозорими [50].

Висновки до підрозділу 2.3

Аналіз сучасних цифрових загроз дозволяє зробити висновок, що дезінформація, «ехо-камери» та кібератаки вже давно переросли рівень звичайних технічних проблем і перетворилися на реальну зброю когнітивної війни. Їхня головна мета - не просто заплутати користувачів, а повністю підірвати довіру до державних інституцій та зробити виборчі процеси хаотичними. В епоху «постправди» фейки, створені за допомогою штучного інтелекту (зокрема, небезпечні технології дипфейків), поширюються з такою швидкістю, що офіційні спростування за ними просто не встигають. При цьому емоційне забарвлення новини для людей стає набагато важливішим за її реальну достовірність.

Не менш серйозним викликом є алгоритмічна поляризація суспільства. Через комерційну логіку соцмереж алгоритми підсовують користувачам лише той контент, який підкріплює їхні власні упередження. У результаті люди опиняються в ізольованих «ехо-камерах». Це призводить до радикалізації настроїв і руйнує можливість нормального політичного діалогу, перетворюючи опонентів на ворогів. Ситуація ускладнюється ще й кібератаками на критичну інфраструктуру, які діють у синергії з інформаційними ударами (як це було під час масштабного збою «Київстару»). Анонімність у месенджерах, особливо в українському сегменті Telegram, дозволяє легко поєднувати реальні інсайди з маніпулятивними вкидами, що безпосередньо впливає на паніку в суспільстві.

Підсумовуючи, можна констатувати, що виклики цифрової епохи неможливо вирішити суто технічними методами, адже вони мають політичну природу. Подальша стабільність системи залежить від здатності держави впроваджувати стратегії цифрової стійкості (digital resilience) та когнітивної безпеки. Окрім традиційного фактчекінгу, потрібно переходити до «пребункінгу» - превентивного навчання громадян методам маніпуляцій. Ефективна протидія вимагає комплексної роботи: від жорсткого правового регулювання соцмереж та посилення кіберзахисту до масових програм із

медіаграмотності. Зрештою, ці загрози мають стати каталізатором модернізації, змушуючи демократичні інститути ставати більш адаптивними та вчитися захищати свій суверенітет у віртуальному просторі.

Висновки до розділу 2

Другий розділ дослідження був присвячений практичному аналізу того, як саме інформаційні технології трансформують ключові інститути та явища в сучасній політиці.

Оцінюючи результати цього аналізу, можна зробити кілька масштабних узагальнень, які демонструють, що цифровізація повністю переписала правила гри як у публічній комунікації, так і безпосередньо в системі державного менеджменту, принісши із собою не лише унікальні можливості, а й безпрецедентні виклики.

Перш за все, дослідження виборчих кампаній чітко показало, що сучасні виборчі технології остаточно перейшли від масового впливу через традиційні медіа до глибокого інструментарію мікротаргетингу. Виборчі штаби тепер змагаються не за ефірний час на телебаченні, а за контроль над алгоритмами та великими даними виборців.

Це змінило і сприйняття часу: концепція постійної виборчої кампанії стала жорсткою реальністю, де політик змушений безперервно бути присутнім у мережі, що часто веде до падіння якості контенту заради швидкості реакції.

Крім того, інтернет зруйнував колишню ієрархію у взаєминах між кандидатом та громадянами, створивши ілюзію прямого горизонтального спілкування. Політики переходять на неформальну мову та стріми, через що емоційна прив'язаність до цифрового образу лідера починає домінувати над тверезим аналізом партійних програм.

Разом із тим, збір Big Data дозволяє штабам створювати психографічні портрети та пропонувати різним групам виборців ізольовані, часто протилежні версії реальності, що замикає людей в ехо-камерах та сильно поляризує суспільство.

З іншого боку, аналіз сфери державного управління продемонстрував, що інформаційні технології здатні еволюційно змінити саму філософію публічної влади. Порівняння традиційної бюрократичної та цифрової моделей управління наочно доводить переваги останньої: перехід від закритих кабінетів до прозорих мережеских платформ дозволяє реалізувати концепцію «держави як платформи».

Автоматизація управлінських циклів мінімізує людський фактор, прискорює надання послуг у режимі 24/7 і створює чіткий цифровий слід, що є потужним ударом по корупції (це підтверджує успішний досвід наших систем ProZorro та Spending.gov.ua).

Завдяки розвитку Open Data звичайні громадяни та журналісти стають реальними суб'єктами контролю, що формує здорову культуру підзвітності влади. Проте тут виникають нові ризики - загроза «фасадної прозорості», коли за горами другорядних даних чиновники приховують реальні центри ухвалення рішень, а також проблема алгоритмічної відповідальності штучного інтелекту, за неупередженістю якого може ховатися нова форма технократичного авторитаризму.

Цифрова епоха сформувала глобальне поле когнітивних та технічних загроз для політичної стабільності. Дезінформація, дипфейки, алгоритмічні інформаційні бульбашки та транскордонні кібератаки сьогодні тісно взаємопов'язані між собою. Вони спрямовані на деструкцію суспільних цінностей та хаотизацію виборів.

В українських реаліях ці виклики мають екзистенційний характер: анонімність комунікації в месенджерах (зокрема в Telegram) дозволяє легко змішувати інсайди з маніпулятивними вкидами для зриву важливих державних процесів, а технічні атаки на критичну інфраструктуру (на кшталт збою «Київстару») миттєво переростають у серйозний політичний чинник, викликаючи паніку в суспільстві.

У підсумку другого розділу можна констатувати, що інформаційні технології успішно трансформують державу із суто контролюючої та

примусової структури на зручного сервісного провайдера, але одночасно роблять суспільство дуже вразливим до прихованих впливів.

Подальша стабільність будь-якої політичної системи залежить від розробки стратегій цифрової стійкості та когнітивної безпеки. Окрім традиційного фактчекінгу, держава має переходити до технологій «пребункінгу» (превентивного навчання громадян методам маніпуляцій).

Ефективний захист вимагає комплексних дій: від законодавчого регулювання соцмереж та посилення суверенного кіберзахисту до масових освітніх програм із медіаграмотності, які допоможуть зберегти демократичні цінності у світі, де політикою починають керувати математичні алгоритми.

РОЗДІЛ 3. ПРАКТИЧНИЙ АНАЛІЗ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПОЛІТИЧНОМУ ПРОЦЕСІ УКРАЇНИ

3.1. Аналіз впровадження електронного врядування та його вплив на публічні послуги в Україні

Практична імплементація електронного врядування в Україні за останні роки перетворилася з технічного експерименту на фундаментальну основу модернізації політико-адміністративної системи. Впровадження цифрових інструментів стало стратегічною відповіддю на застарілість бюрократичних механізмів, високий рівень корупційних ризиків та необхідність підвищення інклюзивності державного управління.

Ключовим етапом цієї трансформації стало створення у 2019 році Міністерства цифрової трансформації України, яке ініціювало перехід до парадигми «Держава як сервіс», де головним суб'єктом є громадянин, а держава виконує роль невидимого, але ефективного провайдера послуг [21].

Технологічний та інституційний базис українського е-врядування. Глибинний аналіз української моделі цифровізації дозволяє виокремити систему «Трембіта» як центральний елемент інтероперабельності. Це система електронної взаємодії, що базується на естонському досвіді (X-Road) і забезпечує безпечний обмін даними між сотнями державних реєстрів.

Функціонування «Трембіти» дозволило реалізувати принцип автоматичного підтягування даних, що радикально скоротило кількість необхідних довідок та копій документів. Як наслідок, політичний процес прийняття адміністративних рішень став більш детермінованим: алгоритм, звертаючись до реєстру, видає результат на основі фактів, а не суб'єктивного рішення чиновника.

Екосистема «Дія» як інструмент політичної суб'єктності громадянина. Найбільш видимим проявом трансформації публічних послуг став бренд «Дія» (Держава і я), що об'єднує мобільний застосунок, веб-портал та мережу

офлайн-центрів підтримки. Україна стала першою державою у світі, яка прирівняла цифрові паспорти до фізичних на законодавчому рівні. Це рішення мало не лише технічне, а й символічне політичне значення, закріпивши пріоритет цифрового права громадянина.

Впровадження таких послуг, як «єМалятко», автоматична реєстрація ФОП та отримання витягів про реєстрацію місця проживання, продемонструвало ефективність децентралізації доступу до послуг [33].

Для детального порівняння ефективності цифрових інструментів та їхнього впливу на державний апарат доцільно звернутися до аналітичних показників (див. табл. 3.1).

Таблиця 3.1. Порівняльний аналіз ключових інструментів е-врядування та їх впливу на політико-адміністративне середовище України

Назва інструменту / Системи	Основна функціональна сфера	Політико-адміністративний ефект	Рівень мінімізації корупційних ризиків
Екосистема «Дія»	Надання адміністративних послуг населенню та бізнесу.	Запровадження сервісної моделі держави; підвищення довіри до влади.	Високий: повна автоматизація без участі чиновника.
Система «ProZorro»	Державні та комунальні закупівлі.	Прозорість використання бюджетних коштів; рівний доступ до ринку.	Критично високий: громадський контроль через відкриті дані.
Портал «Spending.gov.ua»	Моніторинг публічних фінансів та транзакцій.	Реалізація принципу підзвітності влади; фінансовий моніторинг.	Високий: деанонімізація витрат державних установ.
Система «Трембіта»	Міжвідомча взаємодія та обмін даними.	Оптимізація державного апарату; скорочення бюрократичних ланок.	Середній: запобігання фальсифікаціям на етапі обміну даними.
Е-Dem (Е-петиції, Бюджет участі)	Електронна участь та демократія.	Прямий вплив громадян на порядок денний; партисипація.	Низький: інструмент не боротьби з корупцією, а участі.

Аналіз даних таблиці 3.1 свідчить про те, що Україна обрала шлях «радикальної прозорості». Особливо важливим це є для медичної та соціальної сфер, де впровадження електронної системи охорони здоров'я (eHealth) дозволило відстежувати маршрут пацієнта та ефективність використання медичних субвенцій.

Автор може підтвердити, що цифровізація закупівель через ProZorro та звітності через e-Data зробила фінансову діяльність установ повністю прозорою для контролюючих органів та громадськості, що практично унеможливило нецільове використання коштів на місцевому рівні [7].

Цифровізація як чинник національної стійкості в умовах війни. Практичний досвід 2022–2026 років довів, що е-врядування є критичним елементом національної безпеки. Запуск послуг «єВідновлення» для компенсації за пошкоджене майно, цифрова реєстрація ВПО та виплати грошової допомоги через «Дію» дозволили державі зберегти керованість та соціальний зв'язок із мільйонами людей, що опинилися в зоні бойових дій або за кордоном. Це підтверджує, що в Україні цифровізація вийшла за межі «зручності», ставши інструментом збереження функціональності політичної системи в екстремальних умовах [42, с. 50].

Виклики та обмеження практичного впровадження. Попри значні успіхи, процес цифровізації в Україні стикається з низкою об'єктивних викликів. По-перше, зберігається проблема «інформаційної нерівності»: жителі сільських громад та прифронтових територій часто мають обмежений доступ до широкопasmового інтернету, що створює бар'єри для отримання цифрових послуг.

По-друге, інтенсивна концентрація даних в єдиних цифрових вузлах робить систему вразливою до кібератак з боку агресора. Це вимагає постійних інвестицій у кіберзахист та розробку протоколів автономної роботи реєстрів у разі відключення зв'язку. По-третє, існує опір на середній ланці бюрократії, де автоматизація процесів веде до скорочення штату та втрати корупційних рент [15, с. 38].

Додатковим фактором успіху є розвиток Open Data (відкритих даних). Україна стабільно посідає високі місця у міжнародних рейтингах відкритості даних (наприклад, Open Data Inventory). Оприлюднення інформації про власників нерухомості, земельні ділянки, ліцензії та бюджетні витрати у машиночитаних форматах дозволило створити цілу екосистему антикорупційних стартапів (YouControl, Opendatabot), які допомагають громадськості контролювати політичні та економічні еліти.

Підсумовуючи, можна констатувати, що впровадження е-врядування в Україні стало ключовим драйвером трансформації політичного процесу. Цифрові технології не просто замінили папір на електронні форми, а змінили баланс сил між державою та громадянином на користь останнього.

Україна створила унікальний прецедент, коли технологічний прорив став засобом забезпечення політичної прозорості та національної стійкості в умовах глобальних викликів. Подальший розвиток системи має бути зосереджений на подоланні цифрового розриву та посиленні кібербезпеки як фундаментальних умов збереження демократичних інститутів.

Висновки до підрозділу 3.1

Аналіз практичного впровадження електронного врядування в Україні підводить до висновку, що цифровізація вже давно переросла рамки звичайного технічного оновлення кабінетів і стала реальним політичним інструментом.

Створення прозорої системи на базі «Трембіти» та «Дії» - це не просто про зручність у смартфоні, а про принципову зміну балансу сил, де пересічний громадянин нарешті отримує реальну перевагу над чиновником. Вкрай важливим є те, що автоматизація послуг фактично ламає старі корупційні традиції на місцях: коли рішення приймає бездушний алгоритм, а не держслужбовець, простір для хабарів чи маніпуляцій просто зникає.

Такі платформи, як ProZorro або Spending.gov.ua, наочно доводять, що відкриті дані здатні перетворити громадський контроль із формальності на дієву зброю проти зловживань еліт.

Окремо слід підкреслити унікальний досвід України у період криз 2022–2026 років. Саме цифрові сервіси стали головним чинником згуртування, який утримував зв'язок між державою та мільйонами людей, котрі опинилися в окупації, на фронті чи за кордоном.

Те, що ми змогли швидко запустити «Відновлення» чи реєстрацію ВПО в екстремальних умовах, свідчить, що е-врядування в наших реаліях є базовим елементом національної безпеки, а не просто сервісною модною фішкою. Водночас є серйозні внутрішні загрози, які не можна ігнорувати. Це і явна інформаційна нерівність у селах та прифронтових зонах, і тихий, але запеклий опір бюрократів середньої ланки, які банально бояться втратити свої посади та вплив.

Підсумовуючи, можна стверджувати, що український прецедент цифровізації є успішним, але його майбутнє тепер повністю залежить від того, чи зможе держава захистити ці вразливі бази даних від ворожих кібератак і чи зрівняє вона в цифрових правах мешканців великих міст і маленьких селищ.

3.2. Дослідження впливу соціальних мереж на формування політичного порядку денного в умовах воєнного стану

Трансформація стратегічних комунікацій та інституційна роль цифрових платформ у системі державного управління набула критичного значення з початком повномасштабної збройної агресії.

В умовах воєнного стану соціальні мережі перетворилися з допоміжних медійних майданчиків на повноцінну інфраструктуру реалізації державної політики. Традиційні ієрархічні методи інформування населення виявилися недостатньо гнучкими для викликів гібридної війни, що зумовило перехід державних інституцій до моделі прямого цифрового управління.

Соціальні мережі перестали бути лише засобами ретрансляції офіційних повідомлень, перетворившись на автономні простори, де відбувається легітимізація ключових політичних рішень.

Вплив мережевих платформ на політичний порядок денний сьогодні обумовлений їхньою здатністю забезпечувати миттєву комунікацію між державним апаратом і громадянським суспільством, що в умовах воєнного часу є визначальним чинником підтримки соціальної стабільності та довіри до інституцій влади.

Цифрова дипломатія як інструмент зовнішньополітичної дії стала одним із найефективніших засобів просування національних інтересів України на міжнародній арені. Державні інституції, зокрема Міністерство закордонних справ та Офіс Президента, почали використовувати платформу X як інструмент безпосереднього впливу на іноземних політичних акторів та світову громадськість.

Політичні дії в мережі, що включають офіційні звернення до світових лідерів, публікацію візуальних доказів агресії та тегування урядових акаунтів країн-партнерів, сформували нову парадигму публічної дипломатії. Це дозволяє Україні конструювати глобальний порядок денний, оминаючи тривалі протокольні процедури класичної дипломатії. Державна комунікація в мережі змушує іноземні уряди реагувати на запити швидше, оскільки такі звернення потрапляють у поле зору мільйонів користувачів, створюючи потужний суспільний тиск на політичне керівництво країн-союзників щодо надання військової та фінансової допомоги.

Мережевий контроль як механізм антикорупційного та цивільного нагляду став важливим елементом внутрішньополітичного процесу в умовах обмеження роботи деяких традиційних засобів масової інформації. Соціальні мережі перетворилися на інструмент оперативного реагування на управлінські та етичні кризи всередині державного апарату.

Оприлюднення активістами, журналістами та лідерами думок у Facebook фактів нецільового використання бюджетних коштів на місцевому

або центральному рівнях неодноразово призводило до негайних політичних наслідків. Мова йде про кейси щодо закупівель товарів та послуг, які не є пріоритетними для потреб оборони в період дії воєнного стану.

Сила суспільного резонансу в мережевому середовищі змушує органи влади до негайної реакції, що виражається у відставках посадових осіб, проведенні внутрішніх розслідувань та оперативному внесенні змін до нормативно-правових актів, які регулюють порядок використання публічних фінансів.

Таким чином, цифрові мережі виконують функцію незалежного інституційного запобіжника, що забезпечує підзвітність влади навіть у ситуації воєнних обмежень.

Волонтерський рух через механізми цифрової мобілізації став повноправним суб'єктом політичного процесу та ресурсної стабільності держави. Здатність мережевих спільнот за короткий проміжок часу акумулювати ресурси для забезпечення сил оборони сформувала альтернативне джерело легітимності та впливу на державну політику.

Державні органи сьогодні змушені адаптувати свій порядок денний до ініціатив волонтерського сектору, часто інтегруючи його напрацювання в загальнодержавні стратегії та цифрові сервіси. Це свідчить про глибоку трансформацію державного адміністрування від жорсткої вертикалі до гнучкої мережевої моделі управління, де громадянське суспільство через соціальні медіа безпосередньо впливає на пріоритетність логістичного забезпечення фронту та розробку стратегій національної стійкості.

У цьому контексті цифрова активність громадян виступає як форма прямої демократії, що доповнює представницькі інститути.

Протидія деструктивним операціям впливу та захист когнітивного суверенітету населення є окремим критично важливим напрямом державної діяльності в соціальних мережах. В умовах воєнного стану анонімні сегменти месенджерів та соціальних мереж стали основним полем для проведення інформаційно-психологічних операцій з боку агресора. Такі кампанії мають на

меті дискредитацію політичного керівництва, провокування внутрішніх конфліктів та дезорієнтацію цивільного населення.

Політична відповідь держави полягає у розбудові систем стратегічних комунікацій, зокрема через діяльність Центру протидії дезінформації та профільних структур Збройних Сил України. Ці інституції активно використовують мережеві платформи для миттєвої верифікації інформації та формування контрнарративів, що дозволяє утримувати контроль над національним інформаційним простором та запобігати ерозії політичної єдності суспільства.

Еволюція політичної риторики та зміна вимог до публічного політичного лідерства в Україні також є наслідком домінування соціальних мереж у політичному процесі. Сучасні умови вимагають від політиків переходу до методів цифрової щирості, що передбачає використання прямих ефірів, неформальних звернень та швидкої реакції на запити аудиторії в режимі реального часу.

Це докорінно змінює вимоги до професійних якостей публічних осіб, де здатність ефективно комунікувати в мережевому середовищі стає визначальним фактором політичної виживаності та суспільної довіри. Політичний порядок денний тепер формується не лише через офіційні програми, а й через щоденну інтерактивну присутність лідерів у цифровому просторі, що робить політичну культуру більш динамічною, але водночас і більш залежною від короткострокових суспільних настроїв та алгоритмічних трендів платформ.

Підсумовуючи аналіз, слід зазначити, що в умовах воєнного стану соціальні мережі в Україні остаточно закріпилися як інструмент прямої політичної дії. Вони забезпечують безпрецедентний рівень громадського контролю, сприяють реалізації зовнішньополітичних завдань через цифрову дипломатію та виступають головною ареною захисту когнітивної стійкості нації.

Подальший розвиток політичної системи України потребуватиме більш детального законодавчого регулювання статусів цифрових комунікацій та посилення інституційної спроможності держави працювати в умовах постійних мережових викликів, зберігаючи при цьому баланс між свободою слова та вимогами національної безпеки.

Висновки до підрозділу 3.2.

Дослідження того, як соціальні мережі впливають на формування політичного порядку денного під час воєнного стану, приводить до висновку, що цифрові платформи в Україні повністю змінили свій статус.

Вони перетворилися з простих майданчиків для спілкування на критично важливу інфраструктуру, яка безпосередньо забезпечує національну безпеку та керованість держави.

Вкрай показовим є те, як Офіс Президента та Міністерство закордонних справ перетворили мережу X на інструмент прямої цифрової дипломатії. Цей крок дозволив нам конструювати світовий порядок денний в обхід довгих протоколів, створюючи суспільний тиск на іноземні уряди задля отримання зброї, що є унікальним прецедентом у сучасній міжнародній політиці.

На особливу увагу, заслуговує розвиток мережевого контролю як форми прямої демократії всередині країни. В умовах певних воєнних обмежень для класичних ЗМІ саме Facebook став тим простором, де громадянське суспільство зберегло реальні важелі впливу на владу.

Гучні мережеві розслідування щодо нецільових витрат місцевих бюджетів наочно доводять: сила суспільного резонансу в мережі здатна миттєво запускати реальні політичні наслідки - від скасування тендерів до гучних відставок.

Крім того, потужна цифрова мобілізація волонтерського руху фактично змусила державні органи адаптувати свої логістичні стратегії під запити суспільства, що трансформувало управління від жорсткої вертикалі до гнучкої взаємодії.

Цей простір є головним полем когнітивної війни. Анонімні сегменти месенджерів постійно використовуються ворогом для розхитування нашої внутрішньої єдності. І хоча робота Центру протидії дезінформації дозволяє оперативно гасити ці загрози, саме життя в епоху соцмереж виставило нові жорсткі вимоги до політичних лідерів.

Дослідження показує, що сучасний політик тепер повністю залежить від «цифрової щирості» та щоденної інтерактивної присутності в ефірах.

Підсумовуючи, можна стверджувати, що соціальні мережі стали невіддільною частиною нашої стійкості, але головним завданням для держави тепер є пошук тонкого балансу між захистом інформаційного суверенітету та збереженням базових демократичних свобод.

3.3. Виклики кібербезпеки та протидія дезінформації як елемент політичного процесу України

Забезпечення кібербезпеки та системна протидія дезінформації в сучасних умовах трансформувалися з суто технічних завдань у фундаментальну складову політичного процесу України.

В умовах гібридної агресії інформаційно-комунікаційна інфраструктура держави стала об'єктом постійних атак, що мають на меті не лише технічне пошкодження мереж, а й дестабілізацію політичного керівництва, підриг довіри до державних інституцій та маніпулювання суспільною свідомістю.

Кібербезпека в цьому контексті розглядається як гарант суверенітету, оскільки здатність держави захистити власні інформаційні ресурси безпосередньо корелює з її політичною суб'єктністю та стійкістю перед зовнішніми викликами.

Політичний вимір кібербезпеки України характеризується переходом від реактивної моделі захисту до стратегії активного стримування та розбудови цифрової резистентності. Найбільш значущими викликами для політичної системи є атаки на критичну інформаційну інфраструктуру,

державні реєстри та системи електронного врядування. Успішна кібератака на такі ресурси, як портал державних послуг або системи виборчого процесу, може призвести до делегітимізації влади в очах громадян та міжнародної спільноти.

Тому державна політика у сфері кіберзахисту сьогодні інтегрована в загальну стратегію національної безпеки, що підтверджується діяльністю Національного координаційного центру кібербезпеки при РНБО та ухваленням відповідних нормативно-правових актів, що регулюють захист інформаційного простору.

Паралельно із технічними кіберзагрозами, невід’ємним елементом політичної боротьби в Україні стала дезінформація. Вона використовується як інструмент когнітивного впливу, що спрямований на руйнацію суспільного консенсусу навколо стратегічних питань розвитку держави.

Специфіка українського досвіду полягає у протидії складним багаторівневим операціям, які поєднують у собі кіберзлами (наприклад, викрадення конфіденційної переписки політиків) та подальше розповсюдження цих даних через мережу маніпулятивних ресурсів.

Така синергія технічних та інформаційних засобів створює середовище постправди, де політичний порядок денний формується не на основі реальних дій суб’єктів, а навколо штучно сконструйованих наративів, що потребує від держави розробки інноваційних методів захисту інформаційного поля.

З огляду на проведений аналіз та поточні виклики, для вдосконалення політичного процесу та посилення національної безпеки в цифровій сфері пропонуються такі рекомендації.

По-перше, необхідно забезпечити подальшу імплементацію стандартів Європейського Союзу у сфері кібербезпеки та захисту персональних даних до національного законодавства.

Це включає адаптацію положень Директиви NIS2, що дозволить створити єдині високі вимоги до кіберстійкості не лише для державних органів, а й для приватних компаній, що обслуговують критичну

інфраструктуру. Політичне значення цього кроку полягає у зміцненні довіри міжнародних партнерів та створенні безпечного середовища для цифрових інвестицій, що є необхідною умовою післявоєнного відновлення країни.

По-друге, стратегічним пріоритетом має стати розвиток системи національної медіаграмотності як інструменту формування когнітивного імунітету населення. Рекомендується інтегрувати курси з цифрової гігієни та критичного мислення в освітні програми на всіх рівнях, а також проводити регулярні державні інформаційні кампанії для дорослого населення.

Зниження сприйнятливості громадян до дезінформації дозволить нівелювати ефект від ворожих операцій впливу та забезпечити стабільність демократичних процедур, оскільки свідомий виборець є менш вразливим до маніпулятивних технологій у соціальних мережах.

По-третє, доцільним є створення прозорого механізму взаємодії між державними інституціями та великими технологічними компаніями (Big Tech) щодо модерації політичного контенту. Україна має ініціювати розробку міжнародних протоколів, які б зобов'язували соціальні платформи більш оперативно реагувати на поширення дезінформації, що загрожує національній безпеці суверенних держав.

Це включає маркування контенту, згенерованого штучним інтелектом, та розкриття алгоритмів, що формують політичні стрічки новин, з метою запобігання створенню інформаційних ехо-камер, які радикалізують суспільство.

По-четверте, важливо посилити інституційну спроможність органів, відповідальних за стратегічні комунікації. Це передбачає не лише технічне переоснащення Центру протидії дезінформації, а й налагодження постійного діалогу з незалежними експертними середовищами та журналістами-розслідувачами.

Об'єднання зусиль державного та цивільного секторів дозволить створити систему раннього виявлення інформаційних загроз та розробки

ефективних контрнарративів, що базуються на фактах та демократичних цінностях.

По-н'яте, необхідно розширити використання технологій блокчейн та посиленого криптографічного захисту в роботі державних реєстрів та системі надання публічних послуг. Це гарантуватиме неможливість несанкціонованого втручання в дані громадян та забезпечить цілісність інформації, що є фундаментальною умовою для подальшого розвитку електронної демократії та можливого впровадження систем дистанційного волевиявлення у майбутньому.

Таким чином, комплексна реалізація зазначених рекомендацій дозволить не лише захистити цифрові кордони України, а й якісно змінити характер політичної взаємодії.

Перетворення кібербезпеки та протидії дезінформації на системні елементи державного управління сприятиме формуванню прозорого, безпечного та інклюзивного політичного середовища, де інформаційні технології слугуватимуть зміцненню демократичних інститутів, а не їхньому руйнуванню.

Виконання цих завдань вимагає консолідації зусиль влади, експертної спільноти та кожного громадянина, що є запорукою успішної інтеграції України в глобальний цифровий простір.

Висновки до підрозділу 3.3.

Дослідження проблем кібербезпеки та протидії дезінформації в сучасній Україні дозволяє констатувати, що захист цифрових кордонів сьогодні є не просто технічним завданням ІТ-спеціалістів, а базовою умовою збереження політичного суверенітету країни.

В умовах гібридної війни спроби зламати державні реєстри чи запустити чергову масовану хвилю фейків спрямовані на одну головну мету - повністю паралізувати управлінський апарат і посіяти хаос серед громадян. Вкрай

важливим є те, що державна політика у цій сфері нарешті почала переходити до стратегії активного стримування.

Специфіка нашого досвіду, де ворог синхронно поєднує хакерські атаки з когнітивним тиском у медіапросторі, змушує нас шукати абсолютно нові, комплексні рішення для захисту національної стійкості.

На основі проведеного аналізу сформульовано п'ять ключових рекомендацій, що здатні якісно змінити характер політичної взаємодії в цифрову епоху.

По-перше, вбачається за необхідне прискорити адаптацію європейських стандартів, зокрема Директиви NIS2, що дозволить висунути жорсткі вимоги до безпеки не лише державних органів, а й приватних компаній критичної інфраструктури.

По-друге, стратегічним пріоритетом для формування когнітивного імунітету виборців визначено розвиток національних програм із медіаграмотності на всіх рівнях освіти.

Крім того, обґрунтовано доцільність ініціювання Україною створення прозорих міжнародних протоколів взаємодії з компаніями Big Tech для жорсткої модерації шкідливого контенту та обов'язкового маркування штучного інтелекту.

По-третє, пропонується посилити інституційну спроможність Центру протидії дезінформації через постійну співпрацю з незалежними журналістами та експертами. Впровадження блокчейн-технологій та надійних інструментів шифрування даних у реєстрах визначається тією фундаментальною умовою, яка гарантуватиме цілісність інформації й відкриє шлях для безпечного розвитку електронної демократії в майбутньому.

Підсумовуючи, можна стверджувати, що лише таке комплексне поєднання правових, технічних та освітніх засобів дозволить Україні не просто захиститися від поточних загроз, а й побудувати дійсно безпечне й прозоре цифрове середовище.

ВИСНОВКИ ДО РОЗДІЛУ 3.

Комплексний практичний аналіз використання інформаційних технологій у сучасному політичному процесі України дозволяє сформулювати низку узагальнюючих висновків, які відображають глибинну трансформацію всієї системи публічного адміністрування та стратегічних комунікацій.

Проведений аналіз першого підрозділу наочно доводить, що за останні роки впровадження електронного врядування в державі переросло межі звичайного технічного оновлення діловодства й перетворилося на фундаментальну основу модернізації політико-адміністративної системи.

Створення Міністерства цифрової трансформації та практичний запуск взаємодії реєстрів на базі платформи «Трембіта» й екосистеми «Дія» заклали передумови для реалізації сервісної моделі держави. Головним політичним ефектом цих змін стало усунення людського фактора з багатьох етапів ухвалення адміністративних рішень, що автоматично мінімізувало побутові корупційні ризики та знизило рівень бюрократичного тиску на громадян.

Разом із цим, інструменти «радикальної прозорості», такі як платформи ProZorro та Spending.gov.ua, забезпечили суспільство реальними важелями моніторингу та контролю за публічними фінансами, змістивши баланс сил у політичному процесі на користь громадянського суспільства.

Дослідження впливу соціальних мереж на формування політичного порядку денного в умовах воєнного стану підтвердило, що цифрові медіаплатформи остаточно закріпилися як автономна інфраструктура реалізації державної політики та інструмент прямої політичної дії.

У зовнішньополітичному вимірі використання платформи X інституціями влади сформувало нову парадигму публічної дипломатії, яка дозволяє конструювати глобальний порядок денний в обхід тривалих протокольних процедур і створювати дієвий суспільний тиск на іноземні уряди. На внутрішньополітичному рівні соціальні мережі перебрали на себе функцію незалежного інституційного запобіжника.

Сила суспільного резонансу у цифровому просторі, зокрема через поширення антикорупційних розслідувань, здатна запускати негайні управлінські наслідки, скасовувати неперіоритетні тендери та провокувати кадрові ротації навіть в умовах воєнних обмежень для традиційних медіа.

Водночас цифрова мобілізація волонтерського руху продемонструвала перехід від жорсткої управлінської вертикалі до гнучкої мережевої моделі, де громадяни через соціальні медіа безпосередньо коригують державні стратегії логістики та забезпечення сил оборони.

У підсумку аналізу проблем кіберзахисту та протидії дезінформації було визначено, що безпека інформаційних ресурсів сьогодні є ключовим гарантом політичної суб'єктності та когнітивного суверенітету держави. Специфіка сучасних загрозоутворюючих чинників полягає у проведенні складних операцій, які поєднують хакерські атаки на критичну інфраструктуру з подальшим маніпулятивним розповсюдженням даних у медіапросторі з метою дестабілізації суспільства.

Для подолання виявлених деструктивних впливів та наявного цифрового розриву між регіонами у роботі сформульовано п'ять стратегічних рекомендацій. Вони передбачають адаптацію європейських стандартів кіберстійкості

Директиви NIS2, системний розвиток програм із медіаграмотності для формування когнітивного імунітету виборців, ініціювання міжнародних протоколів взаємодії з компаніями Big Tech щодо жорсткої модерації контенту, посилення інституційного потенціалу Центру протидії дезінформації, а також ширше впровадження технологій блокчейн для гарантування цілісності реєстрів.

Тільки таке комплексне поєднання правових, технологічних та освітніх засобів дозволить забезпечити національну стійкість та стабільне функціонування демократичних інститутів України у глобальному цифровому просторі.

ВИСНОВКИ

У кваліфікаційній роботі на основі комплексного аналізу впливу інформаційних технологій на сучасні політичні процеси було детально досліджено як теоретичні виміри цифрової трансформації, так і практичний досвід упровадження новітніх інструментів в українські реалії. Отримані результати дозволяють узагальнити кілька ключових позицій, які відображають характер сучасних змін у політичній сфері.

Аналіз сутності понять «інформаційні технології» та «політичний процес» переконує, що в межах сучасного мережевого суспільства цифрові інструменти переросли роль звичайного технічного супроводу.

Сьогодні вони виступають базовим архітектурним елементом політичної системи, який безпосередньо конструює канали поширення інформації, трансформує механізми ухвалення державних рішень та задає нові формати взаємодії між владними інститутами й суспільством.

Політична конкуренція та мобілізація громадян дедалі чіткіше переносяться у віртуальний простір, який став повноцінною ареною боротьби за владу. Проте цей процес не є однорідним: стрімка цифровізація загострила проблему інформаційної нерівності, коли обмежений доступ до технологій або брак ресурсів у певних груп населення створюють нові лінії соціального розколу.

Вивчення наявних моделей електронної демократії підтверджує, що цифровізація відкриває реальні канали для залучення громадян до безпосередньої участі у державних справах.

Такі інструменти, як онлайн-консультації, електронні петиції та платформи для суспільних обговорень, довели свою спроможність робити роботу державних органів більш прозорою та підзвітною. Водночас практика показує, що самі по собі цифрові платформи не є панацеєю.

Їхня реальна ефективність критично залежить від рівня медіаграмотності суспільства, загальної довіри до інституцій та якості

нормативної бази, яка регулює ці процеси. Відтак, електронну демократію варто розглядати не як заміну традиційним представницьким інститутам, а як інструмент їхньої суттєвої модернізації відповідно до викликів часу.

Окремим вагомим фактором трансформації політичної діяльності стало активне впровадження технологій Big Data та штучного інтелекту. Здатність обробляти колосальні масиви інформації дала змогу політичним акторам глибше розуміти електоральні настрої, прогнозувати поведінку виборців та створювати точкові, персоналізовані звернення.

Разом із тим, алгоритмізація політичного простору принесла серйозні загрози, пов'язані з прихованим маніпулюванням думкою громадян, ризиками для кібербезпеки та приватності персональних даних. Крім того, спостерігається небезпечна залежність традиційних політичних інститутів від алгоритмів глобальних технологічних корпорацій.

Це свідчить про насущну потребу в розробці чітких правових та етичних обмежень для використання систем штучного інтелекту в публічній політиці.

Глибинні зрушення відбулися у сфері виборчих технологій та політичного маркетингу. Поява соціальних мереж та новітніх медіаплатформ забезпечила прямий, безперервний і швидкий зв'язок між лідерами думок та аудиторією.

Сучасні виборчі кампанії вже неможливо уявити без інструментів мікротаргетингу та аналізу цифрових слідів користувачів. Проте зворотним боком цієї доступності стало зростання можливостей для маніпуляцій, радикалізація поглядів всередині замкнених інформаційних «бульбашок» та загальна фрагментація медійного простору, що суттєво ускладнює пошук суспільного компромісу.

Важливим вектором модернізації сучасної держави стає цифровізація управлінських процесів, яка перетворює інформаційні технології на дієвий інструмент підвищення прозорості публічної влади.

Упровадження електронного документообігу, систем відкритих даних, інтеграція публічних реєстрів та запуск цифрових платформ державних

закупівель дозволили суттєво мінімізувати корупційні ризики, скоротити бюрократичну тяганину й зробити роботу владних інституцій підзвітною суспільству.

Завдяки оперативності збору та аналізу даних відчутно зросла і якість самих управлінських рішень. Проте успішність такої трансформації безпосередньо залежить від надійності правових механізмів, захисту персональних даних та зрозумілості алгоритмів, на основі яких функціонують цифрові системи.

За дотримання цих умов технологічні нововведення стають не просто технічною оптимізацією, а базою для відновлення та зміцнення довіри громадян до державних інститутів.

Водночас розвиток цифрового простору актуалізував низку специфічних викликів, серед яких найбільш деструктивний вплив на політичні системи чинять масштабні дезінформаційні кампанії, феномен «ехо-камер» та кіберзагрози.

Сучасні цифрові платформи створили умови для блискавичного тиражування маніпулятивного контенту, а поява штучного інтелекту, здатного генерувати високореалістичні фальсифікати, вивела інформаційно-психологічні операції на кардинально новий рівень.

Ця ситуація ускладнюється алгоритмами соціальних мереж, які штучно закривають користувачів у межах одноманітних інформаційних середовищ. Як наслідок, людина споживає лише той контент, що підкріплює її наявні упередження, що веде до радикалізації поглядів, глибинної поляризації суспільства та руйнування майданчиків для пошуку компромісу.

Крім того, самі кібератаки на критичну інфраструктуру дедалі частіше використовуються як інструмент геополітичного тиску, що вимагає розробки інтегрованих систем кіберзахисту.

У цьому контексті досвід України демонструє унікальні зразки розбудови цифрової держави та впровадження електронного врядування. Заснування профільного міністерства та послідовна реалізація стратегії

«держави у смартфоні» дозволили сформувати принципово нову логіку взаємодії між громадянином та владою.

Переведення ключових адміністративних послуг в онлайн-площину забезпечило їхню доступність та зручність, незалежно від географічного перебування користувача, паралельно знизивши адміністративні бар'єри та побутову корупцію. Особливу життєздатність українська модель цифровізації довела в умовах масштабних криз та воєнного стану.

Здатність цифрових сервісів безперебійно функціонувати в екстремальних обставинах стала вагомим фактором збереження керованості державою та підтримки соціальної стабільності суспільства.

Під час повномасштабної війни принципово змінилася і роль соціальних мереж, які перетворилися на головні канали отримання політичної інформації та інструменти миттєвої суспільної мобілізації. Вони забезпечують координацію волонтерських рухів, оперативне інформування населення та пряму комунікацію між військово-політичним керівництвом і суспільством.

По суті, віртуальний простір став самостійним та надважливим театром інформаційного протистояння. Проте зворотним боком такої динаміки є висока вразливість аудиторії до чуток, панічних настроїв та ворожих психологічних впливів.

Це підтверджує, що захист інформаційного простору сьогодні неможливий без системного розвитку медіагігієни, критичного мислення громадян та постійного вдосконалення державних інструментів стратегічних комунікацій.

Загалом, стійкість сучасної політичної системи безпосередньо корелює з її спроможністю захищати власну цифрову інфраструктуру та протидіяти гібридним загрозам. Кіберпростір остаточно закріпився як вимір політичної та військової конкуренції, де точкові атаки та дезінформаційні хвилі супроводжують традиційні методи протиборства.

Ефективна відповідь на ці виклики не може обмежуватися виключно технічними рішеннями. Вона потребує синергії правових норм, модернізації

національної системи кібербезпеки, глибокої міжнародної співпраці та тривалої роботи над підвищенням загальної інформаційної культури населення.

Підсумовуючи результати дослідження, можна констатувати, що інформаційні технології остаточно стали невід'ємною складовою сучасного політичного процесу, кардинально змінивши принципи діяльності державних органів, політичних партій та інститутів громадянського суспільства.

Цифровізація відкриває колосальні можливості для розвитку демократичних інститутів, оптимізації державного менеджменту та розширення прав громадян.

Водночас вона породжує серйозні ризики маніпуляцій, кібервразливостей та втрати приватності. Проведена робота доводить, що гармонійний розвиток політичної сфери в цифрову епоху можливий лише за умови збалансованого поєднання технологічного поступу з гнучким правовим регулюванням, жорсткими стандартами безпеки та високим рівнем усвідомленості суспільства.

Усі поставлені на початку дослідження завдання були успішно виконані, а сформульовані положення дозволяють комплексно оцінити поточний стан та спрогнозувати подальші тенденції трансформації політичного процесу під впливом глобальної цифровізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналітичний огляд «Інформаційна безпека України під час війни» / Центр стратегічних комунікацій та інформаційної безпеки. 2024. URL: <https://spravdi.gov.ua/analytics/> (дата звернення: 05.06.2026).
2. Баровська А. В. Трансформація державних комунікацій в умовах цифрових викликів. Стратегічні пріоритети. 2023. № 2. С. 15–24.
3. Белоусова Н. В. Політичні маніпуляції в цифрову епоху. Вісник ХНУ імені В. Н. Каразіна. 2022. № 41. С. 77–83.
4. Білорус О. Г. Глобалізм і стратегії глобального розвитку. Київ : Вік, 2021. 430 с.
5. Вебер М. Політика як покликання і професія. Київ : Дух і Літера, 2017. 192 с.
6. Гнатенко О. Політичний маркетинг у соціальних медіа. Сучасне суспільство. 2020. № 1. С. 134–142.
7. Даймонд Л. Розумна сила: деформація демократії та боротьба за владу. Київ : Основи, 2018. 320 с.
8. Данильян О. Г. Інформаційне суспільство та перспективи його розвитку в Україні. Право та державне управління. 2021. № 2. С. 11–17.
9. Дзюба Т. Цифрова дипломатія як інструмент зовнішньої політики. Політичне життя. 2023. № 1. С. 56–63.
10. Дослідження «Digital 2024: Ukraine» / We Are Social & Meltwater. 2024. URL: <https://datareportal.com/reports/digital-2024-ukraine> (дата звернення: 02.06.2026).
11. Дяченко І. О. Еволюція політичних партій у мережевому суспільстві. Політологічний вісник. 2023. Вип. 89. С. 201–210.
12. Звіт про розвиток електронного врядування в Україні за 2023 рік / Міністерство цифрової трансформації України. 2024. URL: <https://thedigital.gov.ua/storage/files/shares/documents/> (дата звернення: 04.06.2026).

13. Звіт про стан реалізації принципів відкритого урядування в Україні за 2022–2024 рр. Київ : КМУ, 2024. 96 с.
14. Інформаційне суспільство в Україні: стан, проблеми, перспективи : нац. доповідь. Київ : НІСД, 2022. 120 с.
15. Кастельс М. Комунікаційна влада / пер. з англ. Київ : КМ Академія, 2013. 608 с.
16. Конвенція про кіберзлочинність (Будапештська конвенція) від 23 листоп. 2001 р. Рада Європи / Верховно Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 01.06.2026).
17. Курбан О. В. Інформаційні війни у соціальних мережах : монографія. Київ : Видавничий дім «Кондор», 2018. 210 с.
18. Лазутін В. В. Цифровізація виборчого процесу: досвід Естонії для України. Порівняльне правознавство. 2021. № 2. С. 90–97.
19. Липченко О. В. Вплив ІТ-технологій на політичну активність молоді в Україні. Політичне життя. 2022. № 3. С. 45–52.
20. Макаренко Є. А. Міжнародні інформаційні відносини. Київ : Либідь, 2002. 350 с.
21. Міжнародний стандарт безпеки інформації ISO/IEC 27001. ISO. URL: <https://www.iso.org/isoiec-27001-information-security.html> (дата звернення: 03.06.2026).
22. Офіційний портал оприлюднення даних про використання публічних коштів. URL: <https://spending.gov.ua/> (дата звернення: 06.06.2026).
23. Офіційний сайт Центру протидії дезінформації при РНБО України. URL: <https://cpd.gov.ua/> (дата звернення: 05.06.2026).
24. Паранчук О. Електронне врядування як чинник демократизації суспільства. Державне управління та місцеве самоврядування. 2021. Вип. 2. С. 112–119.
25. Платформа електронної демократії «E-DEM». URL: <https://e-dem.ua/> (дата звернення: 04.06.2026).

26. Положення про Міністерство цифрової трансформації України : Постанова Кабінету Міністрів України від 18 верес. 2019 р. № 856 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-п> (дата звернення: 01.06.2026).
27. Портал Prozorro. Державні закупівлі України. URL: <https://prozorro.gov.ua/> (дата звернення: 06.06.2026).
28. Постанова Кабінету Міністрів України «Питання Єдиного державного веб-порталу електронних послуг та мобільного додатка Дія» від 4 груд. 2019 р. № 1137 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1137-2019-п> (дата звернення: 01.06.2026).
29. Почепцов Г. Г. Когнітивні війни. Київ : Видавничий дім «Києво-Могилянська академія», 2021. 260 с.
30. Почепцов Г. Г. Психологічні війни. Київ : Ваклер, 2000. 528 с.
31. Про відкритість використання публічних коштів : Закон України від 11 лют. 2015 р. № 183-VIII / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/183-19> (дата звернення: 01.06.2026).
32. Про електронні комунікації : Закон України від 16 груд. 2020 р. № 1089-IX / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1089-20> (дата звернення: 01.06.2026).
33. Про єдиний державний демографічний реєстр : Закон України від 20 листоп. 2012 р. № 5492-VI / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/5492-17> (дата звернення: 01.06.2026).
34. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 лип. 1994 р. № 80/94-ВР / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр> (дата звернення: 01.06.2026).
35. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 01.06.2026).

36. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення: 01.06.2026).

37. Про медіа : Закон України від 13 груд. 2022 р. № 2849-IX / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2849-20> (дата звернення: 01.06.2026).

38. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 01.06.2026).

39. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р. № 447/2021 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/447/2021> (дата звернення: 01.06.2026).

40. Про схвалення Концепції розвитку електронної демократії в Україні : Розпорядження КМУ від 8 листоп. 2017 р. № 797-р / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/797-2017-p> (дата звернення: 01.06.2026).

41. Проєкт «Держава у смартфоні»: концепція та етапи реалізації / Міністерство цифрової трансформації України. URL: <https://thedigital.gov.ua/projects/> (дата звернення: 04.06.2026).

42. Росс А. Індустрії майбутнього. Київ : Наш Формат, 2017. 272 с.

43. Соціальні мережі як інструмент політичної комунікації в умовах війни : аналітична доповідь / за ред. С. О. Гнатюка. Київ : НІСД, 2023. 84 с.

44. Стратегія інформаційної безпеки : затверджена Указом Президента України від 28 груд. 2021 р. № 685/2021 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/685/2021> (дата звернення: 01.06.2026).

45. Суністейн К. Р. Republic.com: роздуми про демократію в епоху інтернету. Харків : Акта, 2010. 256 с.

46. Тоффлер Е. Третя Хвиля. Київ : Всесвіт, 2000. 480 с.

47. Трахтенберг Л. В. Інформаційне суспільство: генезис та правове регулювання. Право та державне управління. 2020. № 4. С. 18–24.
48. Фукуяма Ф. Політичний порядок і політичний занепад. Київ : Наш Формат, 2019. 608 с.
49. Харарі Ю. Н. 21 урок для 21 століття. Київ : BookChef, 2018. 416 с.
50. Цифрова грамотність населення України : аналітичний звіт за 2023 рік / Мінцифра. 2024. URL: <https://osvita.diia.gov.ua/research/> (дата звернення: 04.06.2026).
51. Черевко О. В. Кібербезпека як пріоритет національної безпеки України. Юридичний часопис. 2022. № 4. С. 102–110.
52. Четверта промислова революція : зб. наук. праць / за ред. К. Шваба. Київ : Форс Україна, 2019. 232 с.
53. Чукут С. А. Електронне врядування: світовий досвід та українські реалії. Київ : НАДУ, 2016. 240 с.
54. Шаповал Ю. Політика пам'яті в цифрову епоху. Історичний журнал. 2021. № 2. С. 34–41.
55. Швейцер П. Перемога. Роль таємної стратегії США у розпаді СРСР. Київ : Темпора, 2020. 440 с.
56. Шелест Г. Гібридні загрози та кібербезпека: виклики для України. Політологічні студії. 2023. № 5. С. 12–19.
57. Шумпетер Й. Капіталізм, соціалізм і демократія. Київ : Основи, 1995. 528 с.
58. Юринець О. М. Правове регулювання штучного інтелекту: політичні аспекти. Право України. 2022. № 8. С. 145–158.
59. Якименко Ю. Політичний процес в Україні: цифрові виміри. Рада. 2021. № 4. С. 22–29.
60. Яковенко Н. Вплив соціальних мереж на електоральну поведінку. Держава і право. 2023. № 92. С. 118–125.

ДОДАТКИ

Додаток А

Порівняльний аналіз традиційної та мережевої моделей політичного процесу

Параметри порівняння	Традиційна модель	Мережева модель (ІТ-вплив)
Ключові актори	Держава, партії, офіційні інституції	Мережеві спільноти, блогери, цифрові рухи, ІТ-корпорації
Характер комунікації	Вертикальний (від влади до народу), односторонній	Горизонтальний, інтерактивний, багаторівневий
Швидкість реакції	Низька (бюрократичні процедури)	Миттєва (реакція в режимі реального часу)
Доступ до інформації	Обмежений, цензурований державою	Відкритий, децентралізований, транскордонний
Джерела легітимності	Вибори, правові норми, традиції	Рівень цифрової підтримки, віральність ідей, мережева залученість

Джерела : Традиційна модель [5], [15]

Джерела : Мережева модель (ІТ-вплив) [11], [43]

Додаток Б

Функціональні можливості інструментів електронного врядування в Україні

Назва інструменту / Платформи	Основна політична функція	Вплив на політичний процес
Екосистема «Дія»	Сервісна держава	Зниження побутової корупції, цифровізація взаємодії громадянина і влади
Портал «Prozorro»	Антикорупційний контроль	Прозорість використання бюджетних коштів, громадський нагляд за витратами
Платформа «E-DEM»	Пряма демократія	Реалізація права на електронні петиції та бюджет участі (партисипація)
Портал «Spending.gov.ua»	Фінансова підзвітність	Відкритість державних фінансів для журналістів-розслідувачів та активістів

Джерела: Основна політична функція[12], [28]

Джерела: Вплив на політичний процес[22], [27], [31]

Додаток В

Класифікація інформаційно-технологічних загроз політичній стабільності

Тип загрози	Механізм впливу	Політичні наслідки
Кібератаки на реєстри	Втручання в бази даних, викрадення персональних даних	Делегітимізація державних інституцій, підрив довіри до цифрових сервісів
Дифузія дезінформації	Створення «фейкових новин», робота бот-мереж	Радикалізація суспільства, спотворення волевиявлення, штучна поляризація
Deepfakes (діпфейки)	Створення підроблених відео з виступами політиків	Репутаційні втрати лідерів, провокування міжнародних конфліктів
Алгоритмічні капсули	Штучне обмеження інформації через «бульбашки фільтрів»	Руйнація суспільного консенсусу, неможливість конструктивного діалогу

Джерела: Механізм впливу [1], [29]

Джерела: Політичні наслідки [38], [56]

Додаток Г

Рекомендації щодо зміцнення цифрової стійкості політичної системи України

Напрямок модернізації	Конкретні заходи	Очікуваний результат
Законодавчий	Адаптація стандартів ЄС (NIS2, AI Act)	Створення безпечного правового поля для розвитку ІТ-технологій
Освітній	Запровадження програм медіаграмотності для всіх верств населення	Підвищення стійкості виборців до маніпуляцій та ПІСО
Інституційний	Посилення ролі Центру протидії дезінформації та СтратКому	Оперативне виявлення та нейтралізація ворожих наративів
Технологічний	Впровадження блокчейн-технологій у виборчі та державні процеси	Гарантування цілісності даних та неможливості фальсифікацій