

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет урбаністики та просторового планування

Кафедра політичних наук і права

ЗАТВЕРДЖУЮ



Завідувач кафедри

Перегуда Євген Вікторович

25 червня 2024 року

АТЕСТАЦІЙНА ВИПУСКНА РОБОТА

НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА

Цифровізація політики в контексті ліберально-демократичних цінностей

Виконала Лесик Вероніка Андріївна

(прізвище, ім'я та по батькові повністю)

052 «Політологія»

(спеціальність)

«Політичний менеджмент»

(освітня програма)

Групи ПМ-20

Керівник Стеценко С.В.

(прізвище та ініціали)

Кандидат історичних наук, доцент

Київського національного університету

будівництва і архітектури

(вчене звання, науковий ступінь)

Ідентичність підтверджую

КИЇВ 2024 Р.

ЗМІСТ

ВСТУП

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНА РАМКА РОЗРОБКИ ПРОБЛЕМАТИКИ ЦИФРОВІЗАЦІЇ ПОЛІТИКИ У ПОЛІТИЧНІЙ НАУЦІ

- 1.1. Ключовий понятійно-категоріальний апарат
- 1.2. Концептуалізація владного ресурсу цифрових компаній

РОЗДІЛ 2. ПОЛІТИЧНА СУБ'ЄКТНІСТЬ ІТ-КОМПАНІЙ

- 2.1. Інтерфейс політики і кластера Big-TECH
- 2.2. Політична незалежність держав і «цифрова диктатура»: свобода слова VS інформаційна свобода
- 2.3. Агентивний фактор національних цифрових продуктів в Україні

ВИСНОВКИ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

ВСТУП

Досягнення Перемоги в російсько-українській війні – необхідна умова усталення української незалежності та української національної ідентичності. Це заслін експансіоністсько-вибудованим устремлінням рашистів. Це війна двох світів: світу свободи і демократії проти світового зла і темряви. Неологізм «рашизм» відображає людиноненавистницьку політичну доктрину російського фашизму, що маніпулює ідеологемами: від держави-цивілізації до «руського міра». Росія не полишає спроб принаймні частинні незахідного світу, країнам умовного глобального Півдня, нав'язати власну картину світу, за якою ліберально-демократичні політичні системи знаходяться в кризовому стані, що під питанням залишається саме їх існування.

Рашизм – це не просто ідеологічне опонування демократичному світу, а реальна мілітарна загроза, яка створила вісь зла з агресивними східними автократіями, спонсорує популістські партії та рухи на Заході, поляризуючи протиріччя між країнами. Напередодні Глобального саміту миру у Швейцарії (15-16 червня 2024 року), куди Росію не запросили, світ в черговий раз почув спрямовані проти людяності погрози і абсолютно неприйнятні умови миру з боку рашистів.

Особливу небезпеку за таких політичних реалій становить політична ангажованість і тенденційність політичних акторів інформаційного простору. Провідну роль в ньому відіграють цифрові ІТ-гіганти. Із-за відсутності ефективних правових практик у вирішенні конфліктів в інформаційному полі

вони отримують додаткові важелі політичного впливу. Потужні цифрові компанії беруть на себе роль законодавців, цензорів, навіть поліцейських: визначають регламент угод з користувачами, здійснюють збір персональних даних, застосовують блокування та видалення акаунтів в соціальних мережах.

Актуальність теми обґрунтована необхідністю політологічного дослідження сучасного стану цифровізації політики. В умовах панування цифрових технологій що стали технічною платформою інформаційного

обміну, особливу роль набули потужні ІТ-компанії, виробники цифрової техніки та програмного забезпечення, інтернет-провайдери і особливо компанії – власники інтернет платформ.

Домінуюче місце у світовій індустрії цифрових технологій займає п'ятірка компаній, об'єднаних назвою Big Tech. Саме вони, визначаючи характер інформаційного обміну у світі, роблять бізнес на ключовому принципі ліберальної демократії – свободі слова. Декларативно ці компанії проголошують вільну ринкову конкуренцію і слідування ліберально-демократичним принципам. В дійсності ж йдеться про «цифрову диктатуру» і

перетворення кластера Big Tech в самостійного політичного актора.

Додаткові важелі впливу корпораціям-монополістам надає перехід самої політики в цифрову площину. В умовах цифровізації політики спостерігається тісний взаємозв'язок між органами державної влади та ІТ-корпораціями, коли держава виступає зацікавленою стороною.

Об'єкт дослідження – діяльність ІТ-компаній.

Предмет дослідження – політична суб'єктність ІТ-корпорацій.

Мета полягає у висвітленні інституціоналізації політичної суб'єктності ІТ-корпорацій.

Досягнення поставленої мети передбачає постановку вирішення наступних завдань:

1. визначити теоретичний зміст ключових понять:
демократичні цінності, свобода слова, інформаційна свобода, цифрові технології, кластер Big Tech, цифровий контроль, цифрова диктатура, цифровізація політики.
2. висвітлити порушення демократичних принципів вільного інформаційного ринку з появою монополії цифрових гігантів.
3. показати державу та її структури як зацікавлену сторону в цифровізації політики.
4. охарактеризувати функціональну спрямованість вітчизняних цифрових продуктів, «Дія».

Практичне значення дослідження отриманих результатів зумовлене можливістю використання емпіричного матеріалу та висновків у навчальному

процесі, зокрема щодо проблематики цифровізації політики, в ході підготовки

практичних занять та написанні студентами індивідуальних завдань, доповідей, а також під час навчально просвітницьких заходів, засідань студентського політологічного гуртка.

Структура роботи.

Робота складається зі вступу, двох розділів, що розбиті на підрозділи,

висновку, списку використаних джерел та літератури.

Апробація результатів.

Результати бакалаврської роботи оприлюднені на засіданні студентського дискусійного клубу, Київ, КНУБА, 13 грудня 2023 року.

1.1. Ключовий понятійно-категоріальний апарат.

Процес цифровізації має об'єктивний характер, залежить від глобалізаційних процесів. Однак цьому процесу, як і політичним, так і ринковим відносинам загалом, властиві певні особливості, вади і провали ринку, що потребують державного регулювання та втручання. В більшості країн сучасного світу одним з пріоритетних стратегічних завдань та загально-національних пріоритетів розглядається впровадження інформаційно-комунікаційних технологій (ІКТ) та розвиток елементів цифрового суспільства. Цифрові технології, а також пов'язана з ними громадська та людська діяльність утворюють цифрову сферу сучасного соціуму, яка в нинішніх умовах визначає економічний та інноваційний потенціал держави, рівень освіти та людського розвитку, обумовлює соціальний прогрес, ефективність державного управління та здійснення демократичних процедур.

Цифровізація політики – це процес використання цифрових технологій для покращення управління державними справами, політичними процесами та взаємодії з громадянами. Це охоплює використання інформаційно-комунікаційних технологій (ІКТ), веб-платформ, соціальних медіа, аналітичних інструментів та інших цифрових інструментів для поліпшення якості прийняття рішень, забезпечення відкритості та прозорості управління, залучення громадськості до участі у формуванні політики, ефективного вирішення проблем та виконання завдань держави. Основною метою цифровізації політики є зробити управління більш ефективним, доступним та реактивним на потреби суспільства.

Цифровізація політики може включати в себе такі аспекти, як:

1. Електронне урядування (e-government): використання ІКТ для надання послуг, здійснення взаємодії та спілкування з громадянами і

бізнесом, що спрощує доступ до адміністративних послуг та зменшує бюрократію.

2. Електронна демократія (e-democracy): використання ІКТ для забезпечення громадської участі у політичному процесі, наприклад, шляхом електронних голосувань, онлайн-консультацій та петицій.

3. Відкриті дані (open data): надання доступу до даних державного сектору у відкритому форматі для сприяння прозорості, аналізу та інновацій.

4. Цифрові інструменти аналізу та прийняття рішень: використання аналітичних інструментів та штучного інтелекту для аналізу даних та підтримки прийняття рішень в уряді.

5. Електронна безпека та захист даних: забезпечення безпеки використання та передачі даних в електронному вигляді.

Цифровізація політики є важливим напрямком розвитку сучасних держав, оскільки дозволяє покращити ефективність управління, залучити громадськість до прийняття рішень та забезпечити більшу відкритість та прозорість в управлінні.

Розвиток принципів цифрового суспільства стимулює вдосконалення способів і методів взаємодії в рамках соціально-економічних відносин. Застосування інформаційних технологій дозволяє розширювати комунікаційні процеси, змінює склад і статус їх учасників, принципи просторової взаємодії шляхом мережевого спілкування, підвищує децентралізацію прийняття управлінських рішень в державному і приватному секторі.

На основі аналізу сучасних теоретичних моделей можливо окреслити модель цифрової політики. Елементами моделі є цифрове поле, що впливає на використання певних способів взаємодії цифрових політичних суб'єктів із цифровою інфраструктурою; цифрова інфраструктура – низка технологій/інструментів для інтеграції мереж; мережі користувачів – спільноти громадян, що опановують та застосовують цифрові технології/

інструменти для досягнення спільних цілей, самоврядування; цифрові політичні суб'єкти, що інтегрують ці мережі для здійснення політики.

Цифровізація політики сприяє створенню більш інноваційного та конкурентоспроможного суспільства за рахунок:

- розвитку електронної освіти та підвищенню інформаційної грамотності громадян, що дозволяє забезпечити доступ до знань та можливість саморозвитку;
- створенню умов для розвитку інноваційних технологій та підтримки інноваційних проєктів у різних сферах діяльності;
- забезпеченню доступу до публічної інформації та збільшенню прозорості рішень уряду для громадськості;
- створенню умов для розвитку громадянського суспільства та активізації громадської участі у прийнятті рішень.

Цифровізація політики відіграє ключову роль у формуванні сучасного суспільства, що базується на інформаційних технологіях, і сприяє покращенню якості життя громадян та розвитку демократії.

Цифрове поле, як складова цифрової політики, визначає процедуру формування цифрових політичних суб'єктів, утворення цифрової інфраструктури та механізми інтеграції фрагментованих спільнот.

Цифровізація політики є валентним, нестійким, незавершеним процесом. Це можна пояснити самою природою глобальної цифровізації, що постійно самовдосконалюється та самооновлюється. І, як наслідок, формуються цифрові політичні суб'єкти, здатні до самоорганізації, постійного вдосконалення інструментарію через утворення все більш масштабних спільнот. Тож баланс сил у цифровому світі залежить від миттєвої інтеграції цих спільнот цифровими політичними суб'єктами. Політичні інтеракції стають цифровими, мережевими, що підштовхує усіх учасників політичних процесів сучасності до розбудови мереж і до утворення цифрових політичних рішень. Відповідно, актуальним для політичної науки сучасності є дослідження процесів формування нових цифрових політичних

суб'єктів у новому мережевому середовищі цифрової політики, особливості розбудови мереж суб'єктами цифрової політики для боротьби за владу, застосування влади та впливу на владу, складові цифровізації державної політики [7, с.127].

Необхідно виокремити різні підходи до визначення цифрової політики. Цифрова політика у вузькому значенні розуміється як інтенсифікація використання цифрових технологій у політичних процесах. Таке розуміння не дає змоги пояснити процеси, що викликані цифровізацією політики, оскільки базові цифрові можливості наявні у більшості держав світу. Цифровізація політики у широкому значенні – формування цифрової політичної інфраструктури під впливом дискурсу глобальної цифровізації, що детермінує способи взаємодії цифрових політичних суб'єктів із цією інфраструктурою та зумовлює специфіку утворення мереж для здійснення політики. Цифровізація у цьому широкому значенні призводить до формування політики нового типу – цифрової політики. Цифрову політику визначають як процес упорядкування політичного дискурсу під впливом цифрового поля, що визначає способи використання цифрової інфраструктури. Цю політику здійснюють цифрові політичні суб'єкти, використовуючи потенціал фрагментованих мереж, інтегруючи їх (утворюючи спільноти із слабкими горизонтальними зв'язками) для впливу на процеси визначення та ухвалення політичних рішень. Особливості трансформації політики під впливом цифровізації необхідно визначати через цифрові політичні практики – процес перетворення/перекодування смислів на текст, що у свою чергу породжує нові тексти і нові смисли.

Серед основних факторів, що впливають на процес цифровізації державної політики в зарубіжних країнах, можна виділити:

- активне впровадження нових знань та глобальних інформаційних технологій у всі сфери суспільного життя;
- розвиток громадського суспільства та соціального партнерства в цифровому середовищі;

- особливості створеної у країні моделі ринкової економіки, які виражаються у стимулюванні свободи підприємництва, вільного руху робочої сили, конкурентності ринків;
- ступінь децентралізації влади та ефективність проведення структурної та регіональної політики для поліпшення соціально-економічних умов життя громадян;
- ступінь розвитку економіки країни, який визначає матеріальні можливості людей щодо використання сучасних інформаційних технічних засобів;
- реалізація соціально значущих проектів, що сприяють дотриманню принципів соціальної рівності та справедливості в цифровій економіці [2, с. 4].

Розвиток інформаційно-комунікаційних технологій, програмного забезпечення та відповідної інфраструктури створює певні передумови для формування державної політики цифрового розвитку, заснованої на комплексному підході до вирішення проблем та подолання наявних перешкод, з урахуванням передових світових практик.

1.2. Концептуалізація владного ресурсу цифрових компаній.

Формування образу держави у світі в епоху глобалізації та панування цифрових технологій перестає бути прерогативою політиків, адже число агентів впливу невпинно збільшується за рахунок приватних суб'єктів, зокрема, лідерів думок, інфлюенсерів у соціальних мережах тощо. Однак нові правила політичної гри, що передбачають відкритість та публічність, можна обернути на користь за допомогою продуманої стратегії публічної дипломатії, плоди якої вимірюються не лише позитивним іміджем держави у світі, а й успіхом у просуванні зовнішньополітичних інтересів на міжнародній арені.

В Україні в умовах повномасштабної військової агресії росії наразі формується новий ландшафт загроз національній інформаційній безпеці, зумовлений зростанням кіберзагроз та реалізованих кібератак в умовах наростаючої цифровізації. Це пред'являє принципово інші вимоги до системи забезпечення національної інформаційної безпеки, яка повинна мати властивість не тільки швидкого реагування на поточні загрози, але й мати потенціал для їх запобігання, що насамперед забезпечується високим рівнем цифрової інклюзії та відсутністю цифрової дискримінації та цифрових розривів.

Цифровізація має значний вплив на політичні процеси у сучасному світі, змінюючи способи, якими політика формується, здійснюється та сприймається суспільством. Основні аспекти впливу цифровізації на політичні процеси включають наступні аспекти. Інтернет та соціальні медіа надають можливість політичним лідерам, партіям та громадським організаціям швидко та ефективно спілкуватися з великою аудиторією. Це сприяє поширенню ідей, мобілізації громадян та формуванню громадської думки. Завдяки Інтернету громадяни мають доступ до широкого спектру інформації про політичні події, кандидатів та партії, що сприяє більш обізнаному прийняттю рішень у виборчих процесах.

Цифрові технології створюють нові можливості для громадської участі у політичному процесі через петиції, онлайн-голосування та консультації, що може підвищити легітимність політичних рішень. Використання цифрових інструментів може зробити управління державними справами більш ефективним та прозорим, зменшуючи бюрократію та підвищуючи швидкість реагування на потреби суспільства. Цифрові технології також створюють нові виклики, пов'язані з конфіденційністю та безпекою даних, оскільки збільшується кількість особистої інформації, що обробляється в політичних процесах. У цілому, цифровізація має потенціал покращити політичні процеси, зробити їх більш демократичними та доступними для громадян, але вона також створює нові виклики, які потребують уваги та розв'язання.

Цифровізація є наступним етапом розвитку людської цивілізації, її логічним продовженням. Даний процес охоплює всі сфери людського життя і має на меті змінити їх на краще. Існуюча правова та соціально-політична реальність перебувають в стані активних змін, що є однією з основних складових процесу цифровізації. Визначення цифровізації надане в Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації, відповідно до якої цифровізація – це насичення електронними цифровими пристроями, засобами, системами фізичного світу та налагодження між ними обміну електронним зв'язком, що фактично дозволяє інтегрувати взаємодію віртуального та фізичного, тобто створення кіберфізичного простору [1].

Поширення пандемії COVID-19 також актуалізує перехід держави на електронні адміністративні послуги. Ця обставина пришвидшила процес цифровізації адміністративних послуг й дозволила в коротші терміни налагодити взаємодію між органами державної влади та місцевого самоврядування з набувачами послуг.

Наслідком цифровізаційних процесів є формування сервісної держави, тобто держави, основною функцією якої є захист інтересів та задоволення потреб громадян шляхом їх обслуговування. Формування такого типу держави було однією з основних цілей сучасних адміністративних реформ. Їх мета – підвищення якості надання державних та муніципальних послуг, а також забезпечення високого рівня доступності послуг такого виду [2, с. 242].

Основною умовою формування сервісної держави, є її здатність забезпечити кожного громадянина, кожний господарюючий суб'єкт, кожне громадське об'єднання адміністративними послугами високого рівня якості. При цьому потрібно діяти виходячи з принципів рівності, тобто якість послуг не повинна залежати від особи, яку обслуговують, від місця її знаходження; рівень відмови від обслуговування повинен бути низьким, а рівень доступності до послуг високим [3, с. 89].

І саме в умовах цифровізації, тобто плідної взаємодії між людьми та інтернет-технологіями усі перелічені принципи та вимоги сервісної держави можуть бути реалізованими, адже основною ідеєю цифровізації державних послуг є забезпечення населення послугами адміністративного характеру в електронній формі. В свою чергу, електронні адміністративні послуги – це адміністративні послуги, що надаються заявникам в електронній формі за допомогою інтернет-технологій [4, с. 115]. Крім того, на думку вчених, наразі існують дві взаємопов'язані тенденції, які виникли у процесі цифровізації адміністративних послуг: в основі першої лежить думка про те, що передумовою формування електронного урядування, як нової моделі управління, є саме цифровізація; друга тенденція полягає в тому, що новим способом доступу до інформаційних ресурсів та послуг є можливість переходу від адміністрування до електронного урядування [5, с. 58]. Лише за допомогою належного правового регулювання процедурного механізму стає можливим виконання державою своїх функцій на високому рівні. Це правило є дійсним і у сфері надання адміністративних послуг за допомогою інтернет-технологій

У сучасному світі цифрові технології відіграють все більш важливу роль у політичній діяльності, змінюючи способи, якими політичні лідери спілкуються з громадськістю, як ведуться виборчі кампанії та як формується громадська думка. Одним з ключових аспектів впливу цифрових технологій на політичну діяльність є можливість політичних лідерів та партій ефективно спілкуватися з великою аудиторією через соціальні медіа. Це дозволяє їм швидко реагувати на актуальні події, пропагувати свої ідеї та впливати на громадську думку. Крім того, цифрові технології забезпечують можливість збору та аналізу великих обсягів даних про виборців, що дозволяє підтримувати більш персоналізовані підходи у виборчих кампаніях. До інших аспектів впливу цифрових технологій на політичну діяльність можна віднести підвищення рівня громадської участі через онлайн-петиції та консультації, спрощення виборчих процесів через електронне голосування, а

також підвищення доступності інформації про політичні події та кандидатів для громадськості.

За останні роки спостерігається стрімкий розвиток цифрових технологій, що відкриває нові можливості для політичної діяльності. Однією з головних перспектив розвитку є подальше вдосконалення аналітичних інструментів для збору та аналізу даних про виборців, що дозволить політичним партіям та кандидатам більш ефективно спрямовувати свої зусилля у виборчих кампаніях. Також, можливе подальше зростання впливу соціальних медіа на політичну сферу, що може призвести до зміни традиційних форм комунікації між політичними лідерами та громадськістю. Крім того, важливим аспектом розвитку цифрових технологій в політичній діяльності є забезпечення безпеки та конфіденційності даних, що стає все більш актуальним у зв'язку зі зростанням кількості особистої інформації, що обробляється у політичних процесах. Цифрові технології в політичній діяльності мають великий потенціал для зміни сучасної політичної практики. Вони забезпечують нові можливості для спілкування, мобілізації та впливу на громадську думку. Проте, разом з цим, вони ставлять перед собою нові виклики, такі як забезпечення безпеки та конфіденційності даних, які потребують уваги та вирішення.

РОЗДІЛ 2. ПОЛІТИЧНА СУБ'ЄКТНІСТЬ ІТ-КОМПАНІЙ

2.1. Інтерфейс політики і кластера Big-TECH .

Взаємодія між політикою та кластером великих технологічних компаній (Big Tech) є складним і багатограним процесом, що охоплює різноманітні аспекти від регулятивних питань до впливу на суспільні та політичні процеси. Цей інтерфейс включає як співпрацю, так і конфлікти між державами та великими технологічними компаніями.

Amazon є однією з найбільших транснаціональних корпорацій у світі, відомою своєю широкою діяльністю в електронній комерції, хмарних обчисленнях та наданні цифрових послуг. Заснована у 1994 році Джеффом Безосом, компанія швидко стала лідером у галузі онлайн-торгівлі, надаючи споживачам доступ до мільйонів товарів по всьому світу. Окрім продажу товарів, Amazon активно розвиває свої хмарні сервіси під брендом Amazon Web Services (AWS), які надають потужні обчислювальні ресурси для бізнесу, урядових установ та окремих користувачів. Присутність Amazon у світі включає не лише онлайн-торгівлю, але й створення та управління великими дата-центрами, розробку власних апаратних та програмних рішень, а також активну участь у медіа-бізнесі через платформу Amazon Prime. Така масштабна діяльність робить компанію значним гравцем на глобальних ринках, впливаючи на економіку, технології та соціальні процеси у багатьох країнах, включаючи Україну [35].

Amazon не має великих офісів або складських приміщень в Україні, проте компанія активно працює на українському ринку через свої онлайн-платформи та сервіси. Українські споживачі мають змогу купувати товари з Amazon, користуючись послугами доставки як безпосередньо з міжнародних складів, так і через місцевих посередників. Окрім того, все більше українських підприємств використовують хмарні технології Amazon Web Services для розвитку свого бізнесу, що сприяє зростанню продуктивності та ефективності.

AWS надає українським компаніям доступ до сучасних технологічних рішень, включаючи штучний інтелект, машинне навчання, аналітику даних та

безпекові рішення. Цей фактор є особливо важливим для розвитку технологічного сектору в Україні, де інновації та цифровізація стають ключовими драйверами економічного зростання. Відповідно, присутність Amazon сприяє підвищенню конкурентоспроможності українського бізнесу на міжнародній арені [51].

Amazon має потенціал впливати на політичні процеси в Україні через кілька ключових каналів. Одним із них є контроль над цифровими платформами та інформаційними потоками. Завдяки своїм платформам, таким як Amazon.com і Amazon Prime Video, компанія може впливати на поширення інформації, відбираючи та представляючи контент відповідно до власних політик і бізнес-інтересів. У контексті політичної інформації, це може означати сприяння або обмеження поширення певних новин та політичних матеріалів. Компанія також може впливати на урядові рішення через свої економічні важелі. Amazon є великою корпорацією з величезними фінансовими ресурсами, і вона може використовувати цей вплив для лобіювання сприятливих податкових політик та регуляцій [35]. Наприклад, компанія може вимагати зниження податків або надання інших економічних стимулів в обмін на інвестиції в місцеву економіку чи відкриття нових робочих місць. Іншим важливим аспектом є інвестиції Amazon в місцеву економіку. Компанія може стимулювати розвиток регіонів через інвестиції у технологічну інфраструктуру, створення робочих місць та розвиток місцевих постачальників. Це може мати позитивний вплив на економіку країни, проте водночас такі дії можуть використовуватися як інструмент тиску на уряд для отримання більш сприятливих умов ведення бізнесу [64].

Amazon має розроблені детальні політики щодо контенту, який дозволено розповсюджувати на їхніх платформах. Ці політики стосуються різних аспектів, включаючи захист авторських прав, протидію мові ненависті, дезінформації та іншим формам шкідливого контенту. Наприклад, на платформах Amazon заборонено розміщувати матеріали, що пропагують насильство, дискримінацію або будь-які форми ненависті на основі раси,

етнічного походження, релігії, статі, сексуальної орієнтації чи інших ознак. Ці правила також поширюються на товари, які продаються через платформу. Amazon здійснює ретельний контроль за тим, щоб товари, які продаються через їхні сервіси, відповідали нормативним вимогам і стандартам безпеки. Водночас компанія залишає за собою право видаляти будь-який контент або товари, які порушують ці правила або викликають занепокоєння з боку суспільства. Одним із важливих аспектів політики Amazon є протидія дезінформації. У світі, де інформаційні потоки стають все більш важливими і впливовими, Amazon прагне обмежити поширення неправдивої або оманливої інформації. Це включає як заходи проти відверто неправдивих новин, так і проти контенту, який може вводити в оману споживачів або спричиняти паніку. Такі політики допомагають зберегти довіру користувачів до платформи і забезпечують безпечне середовище для споживачів [35].

Amazon має право цензурувати інформацію, яка вважається небезпечною, некоректною або такою, що порушує встановлені політики. Це може включати як видалення окремих публікацій, так і обмеження доступу до певних видів контенту. Випадки цензури інформації можуть стосуватися різних типів контенту, включаючи політичні матеріали, новини, публікації користувачів та інші види інформації. Цензура політичних матеріалів може виникати у випадках, коли контент містить інформацію, яка порушує законодавство про захист прав інтелектуальної власності, або ж є пропагандистським. Наприклад, під час виборчих кампаній Amazon може видаляти або обмежувати доступ до матеріалів, що містять неправдиву інформацію про кандидатів або політичні партії. Це допомагає зменшити ризики маніпуляції громадською думкою та забезпечити чесність виборчого процесу. У випадку війни цензура інформації стає особливо важливою. Поширення дезінформації під час військових конфліктів може мати серйозні наслідки, включаючи дестабілізацію суспільства, провокації та посилення конфліктів [50].

Amazon може активно видаляти контент, який містить фейкові новини про хід бойових дій, неправдиві повідомлення про втрати серед цивільного населення або пропаганду, що сприяє ескалації насильства. Такі заходи допомагають зберегти стабільність та забезпечити громадську безпеку. Цензура інформації з боку Amazon також може стосуватися матеріалів, які можуть використовуватися у пропагандистських цілях. Це може включати видалення контенту, що пропагує тероризм, екстремізм або інші форми насильницької діяльності. Amazon активно співпрацює з урядовими організаціями та міжнародними інституціями для виявлення та видалення таких матеріалів, забезпечуючи безпеку своїх користувачів та дотримання міжнародних стандартів [51].

Amazon має значний контроль над інформаційними потоками через свої платформи, такі як Amazon Prime Video, Kindle та Amazon Web Services (AWS). В умовах війни між Україною та Росією, контроль над інформацією стає особливо важливим. Наприклад, Amazon може використовувати свої платформи для обмеження доступу до проросійської пропаганди або фейкових новин, що поширюються з метою дестабілізації ситуації в Україні [69]. На платформі Kindle Amazon може обмежувати або видаляти книги та інші матеріали, які містять проросійську пропаганду або неправдиву інформацію про конфлікт. Це допомагає зменшити вплив ворожої пропаганди на українське суспільство та підтримувати інформаційну безпеку. Крім того, AWS може надавати технологічну підтримку українському уряду та військовим структурам для захисту критичної інфраструктури від кібератак. Хмарні сервіси можуть використовуватися для забезпечення надійного зберігання даних, обчислювальних ресурсів для аналізу інформації та підтримки кібербезпеки. В умовах війни такі технології є надзвичайно важливими для захисту інформаційних систем та забезпечення безперебійної роботи урядових та військових структур [65].

У період війни, коли економічна стабільність є критично важливою, залучення великих корпорацій, таких як Amazon, може стати стратегічним

пріоритетом для уряду. Amazon може лобіювати за сприятливі умови ведення бізнесу, наприклад, податкові пільги або спрощення регуляцій для своїх операцій в Україні. В умовах війни, коли економіка країни перебуває під тиском, уряд може бути більш схильним до надання таких пільг у обмін на інвестиції та підтримку економічної стабільності. Це може створити ситуацію, коли політичні рішення ухвалюються з огляду на економічні інтереси великих корпорацій, а не національні інтереси [70].

Amazon, як глобальна корпорація, має значний вплив на міжнародні політичні процеси. У контексті війни між Україною та Росією, компанія може використовувати свій вплив на міжнародній арені для підтримки або протидії певним політичним рішенням. Наприклад, Amazon може лобіювати за посилення санкцій проти Росії або підтримку економічної допомоги Україні з боку західних країн. Цей вплив може бути реалізований через участь у міжнародних бізнес-асоціаціях, взаємодію з урядами інших країн та підтримку політичних ініціатив, спрямованих на допомогу Україні. Такі дії можуть сприяти формуванню більш сприятливих умов для України на міжнародній арені та підтримці її позицій у конфлікті з Росією. Вплив Amazon на політичні процеси в Україні в умовах війни між Україною та Росією є багатограним і включає економічні, інформаційні та політичні аспекти. Компанія може сприяти економічній стабільності та розвитку цифрової інфраструктури, а також відігравати важливу роль у забезпеченні інформаційної безпеки та підтримці міжнародної підтримки України. Однак, водночас важливо враховувати потенційні ризики, пов'язані з економічним та політичним тиском з боку такої потужної транснаціональної корпорації [52].

Amazon відіграє важливу роль в підтримці України під час війни з Росією через свої технологічні ресурси та гуманітарну допомогу. Один із найяскравіших прикладів - підписання Меморандуму про співпрацю між Віце-прем'єр-міністром – Міністром цифрової трансформації України Михайлом Федоровим та Директором з трансформації уряду в Amazon Web Services (AWS) Ліамом Максвеллом. Ця співпраця охоплює сфери цифрової

трансформації, державного управління, цифрової грамотності та інновацій. AWS надав підтримку Україні на суму 75 мільйонів доларів США. Ці кошти були спрямовані на послуги з міграції державних реєстрів та інших важливих державних баз даних до хмарного середовища AWS. Завдяки цим хмарним технологіям державні реєстри продовжують працювати, незважаючи на обстріли та відключення електроенергії, а українці можуть безперервно отримувати державні послуги. Це також забезпечує безпеку всіх даних, оскільки цифрову інфраструктуру не можна знищити ракетами. AWS також надає гуманітарну допомогу та технології, які допомагають українським дітям продовжувати освіту. З перших днів повномасштабного вторгнення AWS надавав значну підтримку Україні, забезпечуючи хмарні технології, що дозволили зберегти важливі державні, банківські та освітні дані. Завдяки міграції даних критична інфраструктура була захищена, і держава продовжила функціонувати [55].

Підтримка з боку AWS включала міграцію близько 100 українських державних реєстрів і критичних баз даних до хмарного середовища AWS. Це дозволило державній цифровій інфраструктурі продовжувати працювати та надавати послуги українцям 24/7, оскільки хмара не може бути знищена ракетами. Така підтримка робить Україну більш стійкою до атак. Міграція до хмарного середовища AWS також допомагає забезпечити безперервність надання державних послуг під час частих ракетних атак і відключень електроенергії. Додаток "Дія" довго зберігає копію системи серверів в AWS і створює щоденні резервні копії з робочого середовища [55]. Це забезпечує безпеку та доступність державних послуг навіть у критичних умовах. Крім міграції до хмарного середовища, AWS співпрацює з Міністерством цифрової трансформації України в сфері ІТ-освіти для українців. У жовтні було запущено пілотний проєкт ITSkills4U, який надає можливість отримати нові навички, пройти сертифікацію AWS та безкоштовно увійти на ІТ-ринок. Понад 11 тисяч українців вже приєдналися до навчальної програми. Ця ініціатива сприяє розвитку ІТ-галузі в Україні, надаючи громадянам нові

можливості для працевлаштування та розвитку кар'єри. AWS також надавав життєво важливі речі для людей, які постраждали від війни, включаючи гаджети для дітей, щоб вони могли продовжувати освіту, та постачання для лікарень. Це підкреслює соціальну відповідальність компанії та її прагнення допомогти країні у скрутний час [55].

Отже, в умовах війни між Україною та Росією Amazon відіграє критично важливу роль у підтримці України через свої технологічні та гуманітарні ресурси. Завдяки підписаному Меморандуму про співпрацю між Міністерством цифрової трансформації України та Amazon Web Services, компанія надає значну підтримку у сферах цифрової трансформації, державного управління, цифрової грамотності та інновацій.

AWS інвестує 75 мільйонів доларів США у підтримку України, що включає міграцію державних реєстрів та інших важливих державних баз даних до хмарного середовища AWS. Ці хмарні технології забезпечують безперервне функціонування державної цифрової інфраструктури навіть під час обстрілів та відключень електроенергії, що робить країну більш стійкою до атак. Важливим аспектом є також забезпечення безпеки даних, адже цифрову інфраструктуру не можна знищити ракетами. Крім того, Amazon активно підтримує гуманітарні ініціативи, надаючи важливі речі для людей, які постраждали від війни, включаючи гаджети для дітей та постачання для лікарень. Освітні проекти, такі як ITSkills4U, надають українцям можливість здобути нові навички та пройти сертифікацію AWS, що сприяє розвитку IT-галузі в країні. Таким чином, Amazon не лише сприяє економічній стабільності та розвитку цифрової інфраструктури України, але й відіграє важливу роль у забезпеченні інформаційної безпеки та підтримці міжнародної підтримки України.

Facebook слугує основною платформою для поширення новин, соціальної взаємодії та політичного дискурсу. Його алгоритми, які визначають пріоритетність контенту на основі залучення користувачів, суттєво впливають на видимість і поширення інформації. Під час українсько-російської війни

Facebook використовувався різними суб'єктами, включаючи уряди, неурядові організації та пересічних громадян, для поширення інформації, пропаганди та дезінформації. Алгоритми, які керують розповсюдженням контенту у Facebook, розроблені таким чином, щоб надавати пріоритет постам, які викликають найбільшу активність. Така пріоритизація може посилювати сенсаційний та емоційно заряджений контент, який часто швидко поширюється під час конфліктів. Дослідження показали, що такі алгоритми можуть ненавмисно сприяти дезінформації та пропаганді, тим самим впливаючи на наративи, які домінують у публічній сфері. Природа цих алгоритмів означає, що контент, який викликає сильну реакцію - як позитивну, так і негативну - має тенденцію до більшої видимості, таким чином викривлюючи інформаційний ландшафт у бік більш екстремальних точок зору.

Уряди України та Росії, а також інші державні та недержавні суб'єкти використовували Facebook як інструмент впливу на громадську думку та поширення своїх наративів. Українські посадовці використовували соціальні мережі, щоб заручитися міжнародною підтримкою та привернути увагу до порушень прав людини. Вони використовували платформу, щоб ділитися останніми новинами та особистими історіями із зон конфлікту в режимі реального часу, прагнучи викликати співчуття та підтримку світової спільноти. На противагу цьому, російські джерела були звинувачені у поширенні дезінформації для виправдання своїх дій та підризу суверенітету України. Це включає широкий спектр тактик, від поширення неправдивих повідомлень про військові дії України до створення фейкових акаунтів, які посилюють проросійські наративи [40].

Роль Facebook у формуванні громадської думки не можна недооцінювати. Такі соціальні мережі, як Facebook, надають простір для дискусій та обміну інформацією, а інформація, якою діляться на цих платформах, може посилювати існуючі упередження, створювати "камери відлуння" та поляризувати думки. Дослідження показують, що під час

українсько-російської війни громадська думка в обох країнах значною мірою формувалася під впливом наративів, представлених у соціальних мережах. Охоплення платформи дозволяє швидко поширювати як достовірну інформацію, так і дезінформацію, що може ускладнити розуміння конфлікту громадськістю [48]. Подвійна роль Facebook у поширенні та контролі інформації підкреслює складний вплив платформи на сучасну війну. З одного боку, вона уможливорює швидку комунікацію та мобілізацію, надаючи голос тим, хто перебуває в зоні конфлікту, і сприяючи глобальній солідарності. З іншого боку, її алгоритми і політика можуть також слугувати поширенню оманливої інформації, формуючи таким чином сприйняття і потенційно загострюючи конфлікти. Таким чином, роль Facebook в українсько-російській війні ілюструє ширший вплив транснаціональних корпорацій на політику та поширення інформації в сучасних конфліктах [40].

Цензура та контроль інформації є критично важливими аспектами впливу Facebook у воєнний час. Участь платформи в різних формах модерації контенту може мати значні наслідки для свободи слова та потоку інформації. Політика модерації контенту Facebook спрямована на видалення шкідливого контенту, зокрема мови ненависті, дезінформації та підбурювання до насильства. Однак ця політика часто є суперечливою, оскільки рішення про те, що є шкідливим контентом, може бути суб'єктивним і залежати від політичного тиску. Проблема полягає в тому, щоб збалансувати видалення справді шкідливого контенту зі збереженням свободи слова [53]. Як українські, так і російські діячі звинувачують Facebook в упередженості та цензурі. Україна критикувала Facebook за те, що він робить недостатньо для стримування російської дезінформації, стверджуючи, що платформа дозволяє поширювати неправдиві наративи, тим самим підриваючи український суверенітет і зусилля, спрямовані на мобілізацію міжнародної підтримки. З іншого боку, Росія звинуватила Facebook у придушенні проросійських наративів, стверджуючи, що практика модерації платформи упереджено ставиться до їхньої точки зору. Ці звинувачення підкреслюють труднощі, з

якими стикається Facebook у збереженні нейтралітету, і можливість того, що його політику можуть сприймати як політично вмотивовану [61].

Практика цензури та модерації у Facebook може мати негативний вплив на публічний дискурс. Користувачі можуть здійснювати самоцензуру, щоб уникнути покарання або видалення з платформи, що може придушити розмаїття думок і знизити ефективність Facebook як простору для відкритого діалогу. Це особливо актуально під час конфліктів, коли доступ до достовірної інформації має вирішальне значення. Необхідність збалансувати модерацію контенту зі збереженням свободи слова є складним і постійним викликом для Facebook. Рішення платформи можуть суттєво впливати на наративи, які домінують у публічному дискурсі, впливаючи як на сприйняття конфлікту, так і на ширшу політичну динаміку [62]. Роль Facebook у цензурі та контролі інформації під час українсько-російської війни ілюструє ширші етичні та практичні виклики, з якими стикаються транснаціональні корпорації в цифрову епоху. Вплив платформи на громадську думку в поєднанні з політикою модерації контенту підкреслює значну владу, яку вона має над поширенням інформації. Наслідки для свободи слова та потоку інформації під час конфлікту є глибокими, що підкреслює необхідність постійного контролю та регулювання діяльності таких потужних організацій [66].

У Facebook було виявлено різні дезінформаційні кампанії, спрямовані як на українську, так і на міжнародну аудиторію. Ці кампанії часто пов'язані з поширенням неправдивих наративів та неправдивої інформації, покликаної заплутати та ввести в оману громадськість. Наприклад, у перші дні повномасштабного вторгнення в лютому 2022 року підтримувані Росією організації поширювали неправдиві повідомлення про те, що українські сили нападають на цивільне населення в регіонах, контрольованих сепаратистами. Ці повідомлення включали сфальсифіковані зображення та відео, які мали на меті зобразити українських солдатів як агресорів, виправдовуючи таким чином російські військові дії. Розслідування, проведене експертами з цифрової криміналістики, показало, що багато з цих повідомлень походять від

скоординованих мереж фейкових акаунтів і сторінок, пов'язаних з російськими інтересами, з метою маніпулювання громадською думкою і сіяння розбрату всередині України та на міжнародному рівні [58].

З іншого боку, Facebook також став потужним інструментом для низової мобілізації та адвокації. Українські активісти та громадські організації використовували цю платформу для організації протестів, обміну інформацією про конфлікт з перших вуст та згуртування міжнародної підтримки. Яскравим прикладом є широке використання Facebook українськими цивільними особами для документування та трансляції реалій війни. Люди публікували відео та фотографії розбомблених будівель, долі біженців і героїчних зусиль місцевих підрозділів оборони. Ці низові зусилля різко контрастували з дезінформаційними кампаніями, пропонуючи правдиві та переконливі розповіді, які здобули широке співчуття та підтримку світової спільноти. Крім того, президент України Володимир Зеленський використовував Facebook для частих відеозвернень до нації та світу, щоб заручитися підтримкою та підтримати бойовий дух [63].

Наративи, поширювані у Facebook, суттєво вплинули на міжнародне сприйняття конфлікту. Західна аудиторія, зокрема, піддавалася впливу суміші новин, думок і пропаганди, формуючи свої погляди на легітимність українського уряду і дії Росії. Наприклад, під час облоги Маріуполя Facebook став полем битви конкуруючих наративів. Російські державні ЗМІ використовували платформу для поширення тверджень про те, що українські військові використовують цивільних як живий щит, тоді як українські джерела публікували докази того, що російські війська атакують цивільну інфраструктуру і скоюють воєнні злочини. Ці суперечливі повідомлення у Facebook вплинули на те, як міжнародна аудиторія сприймала дії обох сторін, що вплинуло на громадську думку та політичний дискурс у західних країнах. Крім того, українські цифрові активісти організовували міжнародні кампанії, такі як «Підтримай Україну», які набули поширення у Facebook і призвели до

глобальних протестів та посилення тиску на уряди з метою підтримки України [41].

Інший показовий випадок - виявлення масових поховань і доказів звірств у Бучі, передмісті Києва, швидко поширилося через Facebook. Українські посадовці та громадяни публікували графічні зображення та відео, які задокументували жахіття, виявлені після відступу російських військ. Ці пости отримали широке розповсюдження і були підхоплені міжнародними ЗМІ, що призвело до сплеску глобального засудження дій Росії та посилення закликів до підзвітності і справедливості. Швидке поширення цих зображень у Facebook відіграло вирішальну роль у формуванні міжнародної реакції, включаючи запровадження додаткових санкцій проти Росії та збільшення військової допомоги Україні [67].

Участь Facebook в українсько-російській війні піднімає важливі етичні та правові питання, що охоплюють питання корпоративної відповідальності, балансу між свободою слова та цензурою, а також ролі транснаціональних корпорацій (ТНК) у міжнародних конфліктах. Ці складнощі підкреслюють значний вплив таких великих платформ, як Facebook, на глобальні події та притаманну їм відповідальність. Як основна платформа для поширення інформації, Facebook несе значну корпоративну відповідальність за те, щоб його послуги не використовувалися для поширення шкідливого контенту або дезінформації [68]. Це передбачає впровадження ефективної політики модерації контенту та співпрацю з фактчекерами та іншими організаціями для перевірки інформації. Наприклад, під час українсько-російської війни Facebook довелося вирішувати делікатне завдання виявлення та видалення неправдивої інформації, яка могла б загострити конфлікт, намагаючись при цьому зберегти простір для вільного вираження поглядів. Балансування між цими обов'язками та необхідністю захисту свободи слова є складним і постійним викликом. Зусилля Facebook у боротьбі з дезінформацією включають співпрацю зі сторонніми фактчекерами для маркування неправдивого контенту та зменшення його поширення, але ці дії часто

викликають критику з різних сторін, що відображає суперечливий характер модерації контенту в умовах високої поляризації [40].

Роль платформи в конфлікті також призвела до різних юридичних проблем. До них належать судові позови, пов'язані з практикою модерації контенту, звинувачення у сприянні порушенням прав людини, а також питання дотримання міжнародних законів і правил. Наприклад, Facebook зіткнувся з юридичною перевіркою щодо того, чи є його нездатність належним чином модерувати шкідливий контент співучастю у поширенні насильства та порушенні прав людини. Вирішення цих правових проблем вимагає ретельного розгляду як національних, так і міжнародних правових рамок. У деяких випадках Facebook звинувачували в тому, що він не діяв достатньо швидко або ретельно для видалення контенту, який підбурює до насильства або поширює дезінформацію, що призводило до потенційних юридичних наслідків. Крім того, дотримання компанією різних національних нормативних актів, які можуть мати суперечливі вимоги щодо цензури та свободи слова, додає ще один рівень складності до її діяльності [53].

Вплив таких ТНК, як Facebook, на громадську думку та політичні процеси викликає ширше занепокоєння щодо впливу корпоративної влади на демократію. Здатність цих корпорацій формувати наративи та контролювати інформаційні потоки може підірвати демократичні процеси та підзвітність. Під час конфлікту, коли точна інформація є критично важливою, контроль, який здійснюють такі платформи, як Facebook, над тим, яка інформація поширюється і посилюється, може мати глибокі наслідки. Наприклад, поширення дезінформації під час українсько-російської війни може ввести в оману громадськість і спотворити процеси прийняття політичних рішень як у країнах, що безпосередньо беруть участь у конфлікті, так і на міжнародному рівні. Ця здатність впливати на публічний дискурс і політичні результати підкреслює необхідність прозорих і підзвітних структур управління в цих корпораціях. Крім того, етичні наслідки алгоритмізованого поширення контенту Facebook підкреслюють суперечність між мотивами отримання

прибутку та суспільними інтересами. Алгоритми, які надають пріоритет залученню, можуть ненавмисно посилювати сенсаційний і роз'єднуючий контент, сприяючи поширенню дезінформації та поляризації громадської думки. Це порушує етичні питання щодо відповідальності платформ соціальних мереж за пом'якшення негативного впливу їхніх бізнес-моделей на суспільство. У зв'язку з цим зростає заклик до посилення регуляторного нагляду та впровадження етичних стандартів для забезпечення відповідності діяльності таких ТНК, як Facebook, ширшим суспільним цінностям і принципам демократичного врядування.

Отже, в контексті впливу Facebook у формуванні громадської думки в умовах українсько-російської війни, очевидно, що ця платформа відіграє значну роль у сучасних інформаційних війнах. Facebook, як потужний інструмент для поширення інформації, має двоякий вплив: з одного боку, він може сприяти поширенню дезінформації та пропаганди, а з іншого – слугувати платформою для мобілізації громадськості та правдивого інформування. Аналіз показав, що алгоритми Facebook часто пріоритизують контент, який викликає сильні емоції, що може сприяти поширенню неправдивих або маніпулятивних повідомлень. У випадку українсько-російської війни, це призвело до значної кількості дезінформаційних кампаній, які намагалися сформувати негативні наративи про дії українських військових і виправдати агресію Росії. Водночас, платформа Facebook стала важливим інструментом для українських активістів та уряду, що використовували її для поширення правдивої інформації, організації протестів та залучення міжнародної підтримки. Публікації та трансляції наживо з місця подій дозволили створити альтернативний до офіційних російських ЗМІ погляд на конфлікт, що допомогло змінити міжнародне ставлення до війни. Етичні та правові виклики, пов'язані з участю Facebook у цьому конфлікті, підкреслюють необхідність балансування між свободою вираження та запобіганням поширенню шкідливого контенту. Роль Facebook у формуванні громадської думки та його

вплив на політичні процеси вимагає підвищеної прозорості, відповідальності та ефективних політик модерації контенту.

Таким чином, Facebook у контексті українсько-російської війни продемонстрував як потенціал для позитивних змін через правдиве інформування та мобілізацію, так і ризики, пов'язані з поширенням дезінформації. Це підкреслює важливість розвитку етичних стандартів і регуляторних механізмів для забезпечення відповідального використання соціальних медіа у сучасних конфліктах.

Розгортання супутникового інтернет-сервісу Starlink компанії SpaceX в Україні є трансформаційним моментом у сучасній війні, ілюструючи, як комерційні технології можуть кардинально впливати на військові та цивільні операції під час конфліктів. На початку російського вторгнення в лютому 2022 року комунікаційна інфраструктура України зазнала серйозних перебоїв через складні кібератаки, організовані Росією. Ці атаки були спрямовані на супутникову мережу Viasat, критично важливий канал зв'язку для українських військових, що фактично підірвало їхню здатність координувати оборонні операції та спілкуватися з міжнародними союзниками.

Усвідомлюючи безпосередню загрозу, яку становили скомпрометовані системи зв'язку, українські урядовці швидко шукали альтернативу, здатну протистояти поточним кіберзагрозам. Starlink, амбітний проект компанії SpaceX із створення супутникового інтернету, став життєво важливим рішенням. За кілька днів перша партія терміналів Starlink прибула в Україну, чому сприяло пряме звернення до Ілона Маска через соціальні мережі. Таке швидке розгортання підкреслило гнучкість і оперативність, які можуть запропонувати рішення приватного сектору в надзвичайних ситуаціях.

Starlink забезпечив надійну та стійку комунікаційну основу, необхідну як для військових операцій, так і для цивільного зв'язку. Для українських військових, особливо для підрозділів, що діють у районах з високим рівнем бойових дій, таких як металургійний комбінат «Азовсталь» у Маріуполі,

Starlink забезпечив безперервний зв'язок. Ця можливість дозволила оточеним військам підтримувати зв'язок зі своїми командирами, забезпечуючи скоординовану оборону, незважаючи на інтенсивний тиск з боку російських військ. Крім того, можливість давати інтерв'ю міжнародним ЗМІ в прямому ефірі із зони конфлікту стала важливим інструментом протидії російським дезінформаційним кампаніям. Таке спілкування в режимі реального часу дозволило українським військовим та урядовцям ділитися нефільтрованими новинами з поля бою, тим самим впливаючи на світове сприйняття та заручаючись міжнародною підтримкою.

Стратегічний вплив Starlink вийшов за межі безпосередніх військових переваг. Він відіграв ключову роль у підтримці морального духу українських цивільних і військових, забезпечивши безперебійний доступ до інформації і каналів зв'язку. Цей зв'язок був особливо важливим у районах, де традиційна інфраструктура була зруйнована або виведена з ладу внаслідок конфлікту. Здатність Starlink надавати доступ до Інтернету через портативні термінали, навіть за відсутності традиційних джерел живлення, підкреслила його корисність у постраждалих від війни регіонах, де підтримка зв'язку є критично важливою як для оперативної ефективності, так і для гуманітарних зусиль. Крім того, стійкість Starlink до спроб радіоелектронної боротьби з боку російських військ продемонструвала її надійність. Децентралізований характер супутникової мережі, що складається з тисяч низькоорбітальних супутників, надзвичайно ускладнив її роботу для супротивника. Навіть коли російські хакери спробували заблокувати систему, інженери SpaceX швидко відреагували, оновивши програмне забезпечення системи, щоб протидіяти цим спробам, тим самим підтримуючи безперебійне обслуговування. Ця адаптивність продемонструвала технологічну досконалість і можливості швидкого вирішення проблем, притаманні підходу SpaceX, встановивши новий стандарт використання комерційних супутникових мереж у військовому контексті [57].

Інтеграція системи Starlink компанії SpaceX у військову стратегію України під час російсько-української війни принесла значні стратегічні і тактичні переваги, глибоко вплинувши на динаміку конфлікту. Одним з найпомітніших аспектів впливу Starlink є його стійкість до російських спроб ведення електромагнітної війни. Російські військові застосовували різні тактики радіоелектронної боротьби, спрямовані на порушення українських комунікацій, які мали вирішальне значення для координації військових операцій і підтримання ситуаційної обізнаності. Традиційні військові системи зв'язку часто намагалися протистояти цим витонченим атакам, але передова технологічна інфраструктура Starlink продемонструвала неабияку адаптивність і надійність [57, 45].

Мережа супутників Starlink на низькій навколоземній орбіті (LEO) виявилася дуже стійкою до перешкод і спроб злому. На відміну від традиційних високоорбітальних супутників, які легше піддаються атакам і виведенню з ладу, децентралізоване угруповання численних низькоорбітальних супутників Starlink надзвичайно ускладнило російським військам завдання виведення мережі з ладу. Така децентралізована архітектура дозволила мережі зберігати функціональність, навіть якщо окремі супутники ставали мішенями, забезпечуючи тим самим безперервне обслуговування, незважаючи на узгоджені зусилля радіоелектронної боротьби. Крім того, здатність SpaceX швидко оновлювати програмне забезпечення на цих супутниках для протидії конкретним загрозам продемонструвала вищу гнучкість і швидкість реагування комерційних супутникових рішень порівняно з традиційними військовими системами зв'язку [45, 39].

Оперативний вплив Starlink на українські збройні сили був значним. Завдяки більш ніж 11 000 станцій Starlink, розгорнутих на різних фронтах, українські війська мають безперебійний зв'язок, що має вирішальне значення для координації складних військових операцій. Таке широке розгортання полегшило зв'язок і обмін даними між різними підрозділами в режимі реального часу, підвищивши загальну ефективність і швидкість реагування

українських військових. Безперервний потік інформації був життєво важливим для виконання скоординованих дій, проведення розвідки та розгортання ресурсів там, де вони найбільше потрібні. Ця здатність надала українським військам значну тактичну перевагу, дозволивши їм ефективно протидіяти російським рухам і стратегіям [39, 36].

Надійна комунікаційна інфраструктура, надана Starlink, відіграла важливу роль у забезпеченні ефективного цивільного управління в зонах конфлікту. У районах, де традиційна інфраструктура була пошкоджена або зруйнована, Starlink дозволив урядовцям і гуманітарним організаціям підтримувати зв'язок з місцевим населенням, координувати зусилля з надання допомоги і управляти основними послугами. Це було особливо важливо для підтримки морального духу населення та забезпечення безперервності управління, незважаючи на конфлікт, що триває. Здатність швидко відновлювати зв'язок у порушених районах підкреслила стратегічну важливість стійких і адаптивних комунікаційних мереж у сучасній війні [39, 36].

Діяльність SpaceX в Україні під час російсько-української війни виходить далеко за межі надання військової підтримки, суттєво впливаючи на ширшу політичну та економічну динаміку. Спочатку SpaceX запропонувала послуги Starlink за мінімальну ціну, отримавши значну фінансову підтримку від США та інших країн-союзників. Ця домовленість продемонструвала потенціал ефективного державно-приватного партнерства в зонах конфліктів, де швидке розгортання передових технологій може надати критично важливу підтримку як військовим, так і цивільним операціям [39]. Однак з розвитком війни позиція SpaceX змінилася. Компанія почала наполягати на тому, щоб уряд США взяв на себе більшу частку операційних витрат, пов'язаних з підтримкою послуг Starlink в Україні. Цей зсув підкреслює складність і залежність, притаманні таким домовленостям, де баланс між комерційними інтересами і геополітичними міркуваннями стає дедалі крихкішим [39].

Одним з найбільш суперечливих аспектів діяльності SpaceX в Україні стало рішення компанії обмежити використання системи Starlink для наступальних військових операцій. Гвінн Шотвелл, президент SpaceX, публічно заявила, що компанія ніколи не мала наміру дозволити використовувати цю технологію в наступальних цілях, що відображає той тонкий баланс, який транснаціональні корпорації (ТНК) повинні проходити між своїми комерційними цілями і геополітичним тиском, з яким вони стикаються [39]. Це рішення мало негайні оперативні наслідки для українських військових, які покладалися на Starlink для різних тактичних і стратегічних цілей, підкреслюючи, як приватні компанії можуть мати значний вплив на політику національної безпеки і оперативну тактику у військових сценаріях.

Ілон Маск, генеральний директор SpaceX, також був суперечливою фігурою в цьому контексті. Його публічні заяви та пости в соціальних мережах часто викликають критику за те, що вони, як видається, підтримують російські наративи. Наприклад, пропозиція Маска щодо «мирного плану», який передбачав повторне проведення референдумів на окупованих територіях під наглядом ООН, визнання Криму частиною Росії та забезпечення нейтралітету України, була сприйнята багатьма як така, що збігається з російськими пропагандистськими зусиллями. Президент України Володимир Зеленський та інші офіційні особи розкритикували нерозуміння Маском складнощів війни та наслідків його заяв [49].

Взаємодія Маска зі світовими політичними лідерами ще більше ілюструє його значний вплив. Незважаючи на напружені відносини з адміністрацією Байдена, Маск продовжує зустрічатися на високому рівні з лідерами таких країн, як Франція, Індія, Ізраїль та Туреччина. Ці зустрічі часто обертаються навколо обговорення технологій, інновацій та стратегічної співпраці, що відображає зростаючу роль Маска як ключової фігури у світовій геополітиці. Однак цей зростаючий вплив також викликає занепокоєння щодо потенціалу однієї особи суттєво впливати на міжнародні відносини та політичні рішення.

Критика на адресу Маска не обмежується його публічними заявами. З'явилися повідомлення про те, що Маск нібито взаємодіє з президентом Росії Володимиром Путіним, які Маск применшує, заявляючи, що їхня взаємодія була обмеженою і нещодавною. Тим не менш, такі звинувачення сприяють сприйняттю Маска як поляризаційної фігури, чиї дії і заяви можуть мати значні геополітичні наслідки [43]. Більше того, коментарі та дії Маска іноді призводили до загострення відносин з іншими країнами. Наприклад, його висловлювання щодо політики «одного Китаю» і Тайваню викликали різку реакцію з боку тайванських чиновників, які розкритикували Маска за його очевидне нерозуміння політичної чутливості регіону. Такі інциденти підкреслюють ширші наслідки зростаючого впливу Маска і необхідність ретельного розгляду його ролі в міжнародних справах [42, 44].

Отже, вплив компанії SpaceX в Україні під час російсько-української війни має далекосяжні наслідки для глобальної політики щодо використання комерційних космічних активів у зонах конфліктів. Цей конфлікт проілюстрував, як доступ до передових комерційних супутникових технологій може суттєво змінити стратегічний ландшафт, дозволяючи країнам, які не мають власного космічного потенціалу, ефективно використовувати сучасні засоби зв'язку та спостереження. Для України розгортання супутника Starlink компанії SpaceX стало трансформаційним, забезпечивши критично важливу комунікаційну інфраструктуру, яка дозволила продовжувати військові і цивільні операції в умовах серйозних перебоїв, спричинених конфліктом.

Одним з найбільш серйозних наслідків є залежність від комерційних структур у забезпеченні критичної інфраструктури у воєнний час, що порушує важливі питання щодо управління і регулювання космічними активами. На відміну від традиційних військових об'єктів, які підлягають суворому державному контролю і нагляду, комерційні космічні об'єкти, такі як ті, що надаються компанією SpaceX, діють в інших нормативно-правових рамках, які можуть не повністю враховувати їх стратегічну важливість у сценаріях конфлікту. Така залежність підкреслює потребу в надійних міжнародних

механізмах, які можуть регулювати розгортання і використання комерційних супутникових послуг під час конфліктів, забезпечуючи доступність і безпеку цих ресурсів.

Український досвід зі Starlink підкреслює потенційну вразливість і ризики, пов'язані із залежністю від єдиного комерційного постачальника основних послуг у воєнний час. Хоча швидке розгортання терміналів Starlink компанією SpaceX принесло негайні вигоди, воно також поставило Україну в залежність від примх і стратегічних інтересів приватної компанії. Наприклад, рішення SpaceX обмежити використання Starlink для наступальних військових операцій відображає складну взаємодію між комерційними інтересами та геополітичним тиском. Це рішення може мати значні оперативні наслідки для українських військових, демонструючи, як комерційні структури можуть здійснювати значний вплив на політику і тактику національної безпеки. Крім того, міжнародне співтовариство має розглянути питання про те, як забезпечити безпеку і стійкість цих комерційних космічних об'єктів. Під час конфлікту здатність Starlink протистояти російським спробам електромагнітної війни та кібератакам мала вирішальне значення. Здатність SpaceX швидко адаптуватися і протистояти цим загрозам підкреслила технологічну досконалість комерційних космічних рішень. Однак це також вказало на необхідність міжнародних стандартів і спільних зусиль для захисту цих активів від ворожих дій, забезпечення їхньої надійності в критичних ситуаціях. На геополітичний ландшафт також впливає помітна роль таких постатей, як Ілон Маск, чиї рішення і публічні заяви можуть мати значні глобальні наслідки. Суперечлива взаємодія Маска з російськими наративами та його пропозиції щодо конфлікту викликали значні дискусії та критику. Ця ситуація підкреслює необхідність більшої уваги і, можливо, нових регуляторних заходів для управління впливом впливових осіб та їхніх компаній на міжнародну безпеку і політику.

Таким чином, діяльність SpaceX в Україні та ширші дії Ілона Маска ілюструють значний вплив, який ТНК та їхні лідери можуть мати на глобальну

політику та економічну динаміку. Приклад Starlink в Україні висвітлює потенційні переваги та виклики державно-приватного партнерства в зонах конфліктів, тонкий баланс між комерційними інтересами та геополітичним тиском, а також значний вплив, який впливові особи можуть мати на формування міжнародних відносин. Оскільки роль ТНК у світових справах продовжує зростати, важливо критично оцінювати їхні дії та ширші наслідки для міжнародної стабільності та безпеки.

Залучення Microsoft до політичних процесів в Україні проявляється у широкій співпраці з різними державними органами та активній участі у формуванні національної політики. Одним із ключових напрямків цієї співпраці є державно-приватне партнерство. Наприклад, Microsoft співпрацює з Міністерством цифрової трансформації України з метою розвитку цифрової інфраструктури країни. Ця співпраця зосереджена на наданні технологічних рішень для підвищення ефективності та стійкості уряду, особливо в умовах триваючого конфлікту. Прикладом такої співпраці є участь корпорації Майкрософт у проєкті «Дія» - платформі електронного урядування, започаткованій українським урядом. Дія, що в перекладі з української означає «Дія», має на меті оцифрувати державні послуги, зробивши їх більш доступними для громадян. Хмарні технології та досвід Microsoft відіграли важливу роль у розробці та підтримці цієї платформи, яка пропонує широкий спектр послуг, від цифрових паспортів до реєстрації бізнесу. Це партнерство підкреслює відданість Microsoft підтримці зусиль України у сфері цифрової трансформації [56].

Microsoft бере участь у консультативних заходах, беручи участь у форумах та дискусійних групах, які впливають на прийняття рішень щодо національної політики. У 2020 році корпорація Майкрософт об'єднала зусилля з Радою національної безпеки та оборони України для протидії загрозам кібербезпеки. Ця співпраця передбачала обмін досвідом та ресурсами для зміцнення кіберзахисту України, що є критично важливим з огляду на посилення кіберзагроз з боку Росії під час конфлікту. Участь корпорації

Майкрософт у таких стратегічних ініціативах високого рівня підкреслює її роль як ключового гравця в політичних процесах в Україні [46].

Вплив Microsoft на формування політики та управління в Україні є значним, що зумовлено її технологічними можливостями та економічною потужністю. Яскравим прикладом є роль компанії у формуванні політики кібербезпеки України. У відповідь на зростаючу кількість кібератак, особливо з російських джерел, Microsoft надала життєво важливу підтримку в розробці та впровадженні комплексних стратегій кібербезпеки. Ця участь включає в себе розгортання передових рішень безпеки, проведення оцінки загроз та пропонування навчальних програм для українських фахівців з кібербезпеки. Показовим прикладом є допомога Microsoft після кібератаки NotPetya у 2017 році, яка серйозно підірвала українську інфраструктуру. Корпорація Майкрософт співпрацювала з українською владою, щоб підвищити її кіберстійкість, надаючи передові рішення для захисту від загроз та відновлення. Це партнерство допомогло Україні оговтатися від атаки та зміцнити свій захист від майбутніх кіберзагроз [37].

Окрім кібербезпеки, корпорація Майкрософт відіграла вирішальну роль у приведенні української політики захисту даних у відповідність до міжнародних стандартів. У міру того, як Україна наближається до європейської інтеграції, приведення її законодавства про захист даних у відповідність до Загального регламенту про захист даних Європейського Союзу (GDPR) набуває все більшого значення. Досвід корпорації Майкрософт у сфері захисту даних та дотримання вимог законодавства був неоціненним у цьому процесі. Компанія працювала з українськими регуляторами над розробкою та впровадженням законодавства, яке відповідає стандартам GDPR, забезпечуючи захист персональних даних та сприяючи створенню безпечного цифрового середовища [47]. Вплив Microsoft поширюється на економічну політику, яка сприяє розвитку цифрової економіки. Виступаючи за політику, яка заохочує інновації, підтримує стартапи та розвиває цифрові навички, Microsoft допомагає створити сприятливе середовище для

технологічного прогресу. Ця підтримка має вирішальне значення для економічного відновлення та зростання України, особливо у світлі триваючого конфлікту. Наприклад, ініціативи Microsoft у сфері цифрової освіти та навчальних програм мають на меті забезпечити українську робочу силу необхідними навичками для цифрової епохи, тим самим підвищуючи конкурентоспроможність та економічну стійкість країни [59].

Підтримка Microsoft ініціатив з цифрової трансформації та електронного урядування в Україні є наріжним каменем її впливу в країні. Зусилля компанії значно підвищили ефективність, прозорість та доступність державних послуг. Одним з найвідоміших проєктів є вищезгадана платформа «Дія». Ця ініціатива електронного урядування, що підтримується хмарними рішеннями Microsoft Azure, дозволяє громадянам отримати доступ до понад 50 державних послуг онлайн, включаючи отримання цифрового посвідчення особи, сплату податків та доступ до соціальних послуг. Успіх платформи є свідченням трансформаційного впливу технологій Microsoft на державне управління. На додаток до підтримки інфраструктури, Microsoft запустила широкі навчальні програми для підвищення цифрової грамотності серед державних службовців. Ці програми охоплюють різні аспекти цифрового врядування - від кібербезпеки та управління даними до використання хмарних інструментів. Розширюючи цифрові можливості державних службовців, Microsoft гарантує, що український уряд зможе ефективно використовувати нові технології для покращення надання послуг та управління [60].

Вплив Microsoft також поширюється на освітній сектор, де вона співпрацює з навчальними закладами для інтеграції цифрових інструментів у навчальні програми. Під час пандемії COVID-19 та в умовах конфлікту, що триває, Microsoft надала безкоштовний доступ до свого пакету Office 365 для підтримки дистанційного навчання. Ця ініціатива допомогла зберегти безперервність освіти для мільйонів учнів по всій Україні, продемонструвавши вирішальну роль цифрових рішень у забезпеченні стійкості під час кризових ситуацій. Microsoft підтримує інноваційні центри та

технологічні інкубатори, які сприяють розвитку місцевих стартапів і технологічних підприємств. Компанія надає доступ до передових технологій, менторства та можливостей фінансування, сприяючи розвитку технологічної екосистеми в Україні. Наприклад, програма Microsoft для стартапів відіграє ключову роль у допомозі українським технологічним компаніям масштабувати свою діяльність та впроваджувати інновації. Ці зусилля є життєво важливими для стимулювання економічного зростання та технологічних інновацій, особливо у складні часи [38].

Під час українсько-російської війни Microsoft відіграла ключову роль в управлінні інформаційними потоками, балансуючи між потребою у свободі вираження поглядів та необхідністю запобігти поширенню дезінформації та захистити національну безпеку. Підхід Microsoft до контролю над інформацією в цей період включав поєднання модерації контенту, стратегічного партнерства та дотримання міжнародних і місцевих норм. Одним із ключових аспектів ролі Microsoft була боротьба з дезінформацією. Дезінформаційні кампанії, часто організовані державними суб'єктами, викликали значне занепокоєння під час конфлікту. Microsoft розгорнула програму "Захист демократії", яка має на меті захистити демократичні процеси від кіберзагроз та дезінформації. Ця програма передбачає використання передових інструментів штучного інтелекту для виявлення та зменшення поширення неправдивої інформації на своїх платформах, включаючи соціальні мережі та комунікаційні інструменти, такі як LinkedIn і Teams [54].

Microsoft також співпрацює з українським урядом та міжнародними організаціями для посилення кібербезпеки та інформаційної цілісності. Наприклад, у 2022 році Microsoft тісно співпрацювала з Міністерством цифрової трансформації України, щоб захистити цифрову інфраструктуру країни від кібератак та дезінформаційних кампаній. Це партнерство передбачало не лише технологічну підтримку, а й стратегічні консультації щодо найкращих практик управління інформацією та безпеки. Крім того, корпорація Майкрософт дотримується місцевих та міжнародних норм щодо

контролю над інформацією. Це включає дотримання санкцій та експортного контролю, які обмежують доступ до певних технологій та інформації для суб'єктів, пов'язаних з російською державою. Привівши свою діяльність у відповідність до цих нормативних вимог, Microsoft зробила свій внесок у ширші зусилля, спрямовані на обмеження впливу ворожих інформаційних операцій під час конфлікту [54].

Реальні приклади участі Microsoft в інформаційній цензурі та регулюванні під час українсько-російської війни ілюструють практичне застосування її механізмів і стратегій. Одним із яскравих прикладів є видалення російського державного медіа-контенту з платформ Microsoft. У відповідь на війну компанія Microsoft вжила рішучих заходів для обмеження поширення пропаганди та дезінформації, заблокувавши доступ до RT (Russia Today) і Sputnik, двох відомих російських державних ЗМІ, у своїй пошуковій системі Bing і магазині додатків. Цей крок став частиною ширшої ініціативи технологічних компаній, спрямованої на зменшення впливу дезінформації, що фінансується державою [46]. У координації з Google та Meta (колишня назва Facebook) Microsoft допомогла виявити та ліквідувати мережі фейкових акаунтів та веб-сайтів, які поширювали неправдиву інформацію про війну. Ці кампанії часто мали на меті посіяти розбрат серед українського населення та підірвати довіру до уряду. Використовуючи свій досвід у сфері кібербезпеки та технологічні ресурси, Microsoft відіграла ключову роль у нейтралізації цих загроз та забезпеченні більш безпечного інформаційного середовища [47].

Отже, роль Microsoft у регулюванні політичних процесів в Україні в умовах війни з Росією є значною та багатогранною. Компанія виявилася ключовим партнером українського уряду в різних аспектах, від цифровізації урядових послуг до забезпечення кібербезпеки. Співпраця з Міністерством цифрової трансформації та участь у проектах, таких як платформа «Дія», демонструють, як технологічні рішення Microsoft сприяють підвищенню ефективності державного управління та зміцненню довіри громадян до уряду.

Майкрософт також відіграє важливу роль у формуванні політики кібербезпеки в Україні, допомагаючи розробляти та впроваджувати стратегії для захисту критичної інфраструктури від кіберзагроз. Зокрема, після кібератаки NotPetya, компанія надала життєво важливу допомогу в покращенні кіберстійкості України, що є важливим для підтримки національної безпеки в умовах триваючого конфлікту. Що стосується регулювання інформаційних потоків, Microsoft застосувала кілька механізмів, включаючи модерацію контенту, блокування дезінформації та співпрацю з іншими технологічними компаніями для протидії кіберкампаніям з дезінформації. Приклади блокування доступу до російських державних ЗМІ, таких як RT та Sputnik, на своїх платформах, свідчать про рішучість компанії в обмеженні поширення пропаганди, яка може дестабілізувати політичну ситуацію в Україні. Вплив дій Microsoft на місцеве населення та політичний клімат є значним. Завдяки цифровізації урядових послуг та покращенню кібербезпеки, компанія допомогла зберегти функціональність державних інституцій, підвищити довіру громадян до уряду та забезпечити безперервність надання публічних послуг. Це сприяло зміцненню політичної стабільності та соціальної згуртованості в Україні.

Можна стверджувати, що вплив транснаціональних корпорацій, таких як Microsoft, на політичні процеси та управління інформаційними потоками в умовах війни є надзвичайно важливим. Досвід України демонструє, як технологічні компанії можуть не тільки сприяти економічному розвитку та модернізації державних послуг, але й відігравати критичну роль у забезпеченні національної безпеки та інформаційної стійкості. Уроки, отримані від цієї співпраці, можуть служити зразком для інших країн, що стикаються з подібними викликами.

2.2. Політична незалежність держав і «цифрова диктатура»: свобода слова VS інформаційна свобода

У науковому оточенні виокремлюються певні етапи інформатизації: електронізація, комп'ютеризація, медіатизація і, нарешті, інтелектуалізація – процес розвитку здатності суспільства до породження і сприйняття знань, тобто підвищення інтелектуального потенціалу, включаючи використання засобів штучного інтелекту. Головною метою соціальної інформатизації є побудова інтелектуального суспільства – суспільства, побудованого на знаннях.

У сучасному законодавстві, зауваження вчених вказують на методологічну невірність у використанні терміну "електронний" – електронна демократія, електронна економіка, електронна комерція, електронна послуга, електронна культура, електронна освіта, електронна медицина. Це мовне запозичення не єдине, поруч з ним увійшли "цифровізація" (диджіталізація, дигітилізація), і його похідні – цифрова демократія, цифровий підпис, цифрові права, а також "кібер-" – кібердемократія, кібербезпека, кіберпростір, кіберзлочини тощо.

Незважаючи на це, терміни "електронна демократія", "електронна комерція", "електронна послуга" та інші вже стали неодмінною частиною наукової і політико-правової лексики. Їх активно використовують у соціальних, політичних, правових науках, а також в міжнародному праві та законодавстві багатьох розвинених країн. Крім того, термін "електронний" часто замінюється англійським префіксом "е-": е-демократія, е-голосування, е-комерція, е-послуга, е-освіта, е-медицина тощо.

У нашій країні довгий час е-демократію і е-урядування розглядали як синоніми, надаючи перевагу останньому. Згаданий Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" не включав поняття електронної демократії. Основні напрями е-демократії визначалися Концепцією розвитку електронного урядування в Україні, Стратегією державної політики сприяння розвитку громадянського суспільства, та Планом дій ініціативи "Партнерство "Відкритий Уряд". Однак у листопаді 2017 року Кабінет Міністрів України схвалив Концепцію розвитку електронної демократії до 2020 року та План заходів щодо її реалізації до кінця 2018 року, які розроблені Державним агентством з питань електронного урядування України спільно з Коаліцією розвитку електронної демократії.

Затверджений план передбачає створення нормативно-правового забезпечення для електронної демократії, що включає норми для забезпечення належного функціонування електронних інформаційних ресурсів органів влади, вдосконалення механізму подання та розгляду електронних петицій, підвищення участі громадян у процесах прийняття рішень через запровадження інструментів електронних консультацій, створення основ для електронного голосування та удосконалення принципів розвитку відкритих даних.

Світовий досвід показує, що е-демократія визначається як необхідний компонент електронного урядування, нарівні з постачанням е-публічних послуг. Це висновок можна зробити на основі аналізу Рекомендації Комітету Міністрів країн-членів Ради Європи з е-урядування, яка визначає е-демократію як використання ІКТ в демократичних процесах, що сприяє участі, ініціативності та залученню громадян на різних рівнях публічного життя. Важливим є також покращення прозорості прийняття демократичних рішень та підзвітності демократичних інститутів, а також забезпечення чутливості органів влади до звернень громадян.

Рекомендації Ради Європи визначають 20 принципів е-демократії, серед яких основне завдання є посилення демократії та демократичних процесів, а також поширення демократичних цінностей. Вони підкреслюють, що е-демократія повинна бути інтегрованою з традиційними процесами демократії та базуватися на гуманістичних, соціальних, етичних та культурних цінностях суспільства, в якому вона розвивається. Також важливо, що е-демократія тісно пов'язана з "добрим урядуванням", що передбачає ефективне управління на основі результативності, участі, прозорості та підзвітності.

У Європейських країнах інформація, оприлюднена електронними засобами, розглядається як складова е-послуг і вважається необхідною для забезпечення участі громадян у владних процесах та реалізації їх законних прав і свобод. Україна також рухається у цьому напрямку, але стикається зі складнощами, зокрема, з популізмом та корупцією. Потреба в правильному використанні відкритих даних стає важливою у розвитку електронної демократії в Україні.

Варто зазначити, що успіх е-демократії не залежить від кількості чи якості використовуваних технологій. Відповідальність за впровадження технологій має лежати на інституціях, які відповідають за політику е-демократії. Світовий досвід показує, що країни, де е-демократія успішно функціонує, такі як Естонія, Сполучене Королівство, Німеччина та Швеція, активно залучають громадян у політичні процеси, що робить їх більш прозорими та доступними для участі громадян.

Цифрова диктатура є темою, що на сьогоднішній день набула дуже актуального значення. Вже у 1980-х роках Й. Масуда в своїй праці "Комп'ютопія" попереджав світ про небезпеку "руху у напрямі контрольованого суспільства". Він стверджував, що людство стоїть перед вибором між двома сильно контрастуючими майбутніми моделями – "Комп'ютопією", що означає демократичне, правове інформаційне суспільство, та "автоматизованою державою"[71]. Професор Масуда намагався знайти пояснення в історії виникнення технологій, оскільки у перших роках їхнього застосування комп'ютери використовувалися, в першу чергу, військовими і іншими урядовими структурами. Таке використання загрожувало "зазіханням на індивідуальну самотність та кризою підконтрольності.

Сучасний приклад реалізації цих страшних прогнозів можна побачити в Китаї. У червні 2014 року Державна рада Китаю опублікувала "Проект плану зі створення системи соціального кредиту довіри, 2014–2020", метою якого стало формування рейтингу благонадійності жителів Китаю. Вже в 2007 році були закладені передумови для формування систем соціального контролю, коли було опубліковано "Деякі зауваження канцелярії Держсекретаря КНР про створення системи соціального кредитування". Основою для проекту була система скорингу – оцінки платоспроможності, яка є поширеною світовою практикою. Головною метою проекту стало "використання міжнародного досвіду, вдосконалення системи сканування щодо кредитування, оподаткування, виконання контрактів, якості продукції".

Однак в 2014 році було внесено не лише зміни до суб'єктного складу – з компаній на громадян Китаю та всіх мешканців, а й до підходів та цілей програми. Система "соціального кредиту довіри" передбачає відстежування і оцінку поведінки людей, а також формування рейтингу довіри в реальному часі, який буде прив'язаний до внутрішнього паспорту і знаходитись у вільному доступі в централізованій базі даних в Інтернеті.

Тестовий режим системи було впроваджено приблизно в тридцяти містах Китаю, зокрема в місті Жунчен в провінції Шаньдун. Всім жителям міста (670 тисяч осіб) було надано вихідний рейтинг 1000 балів, який змінювався в залежності від їхньої поведінки. Інформація про життя і діяльність громадян надходить з муніципальних, комерційних, правоохоронних та судових органів в єдиний інформаційний центр, де вона обробляється за допомогою технології "Великі Дані". В цілому рейтинг формується на основі аналізу 160 тисяч різних параметрів з 142 установ. Проект передбачає преміювання за доноси – громадянину, що повідомив куди слід про "не доброчесні" дії свого сусіда, додається як мінімум п'ять балів.

Над впровадженням цієї системи працювали китайські корпорації, зокрема, компанія China Rapid Finance, партнер Tencent, розробник месенджера WeChat з базою в понад 850 мільйонів користувачів. Активно сприяє системі торгівельний Інтернет-гігант Alibaba, яким в Китаї користуються більше половини Інтернет-користувачів. Рейтингова система Alibaba, Sesame Credit, що вже другий рік надає користувачам бали, враховуючи їх споживчу поведінку. Sesame ранжує клієнтів за шкалою від 350 до 950 балів і надає переваги користувачам в залежності від їхнього балу.

У 2016 році Державна рада Китаю уточнила документ під назвою “Механізми попередження та покарання людей, схильних до порушень”, в якому передбачено санкції для людей з низькими рейтингами. Такі санкції включають заборону на роботу в державних установах, відмову у соціальному забезпеченні, підвищений контроль на митницях, обмеження у роботі в харчовій і фармацевтичній промисловості, а також обмеження на авіаквитки та нічні поїзди, доступ до луксових готелів і ресторанів, а також заборону на навчання дітей у дорогих приватних школах.

Система також оцінює рейтинги юридичних осіб за відповідність юридичним, екологічним та фінансовим нормам, і ті, що отримують високий рейтинг, користуються пільговими умовами оподаткування та кредитування.

Така система не обмежується лише населенням, вона також поширюється на владні структури. Наприклад, партійна школа при Комітеті Комуністичної партії Китаю провінції Сичуань уклала угоду з Університетом електроніки і технологій КНР щодо створення першої в країні системи рейтингів і оцінки надійності для чиновників низового рівня. Система, яку назвали “Розумна червона хмара”, використовує технології штучного інтелекту та великі дані для аналізу даних про чиновників.

Такі кроки викликали дискусії щодо того, чи може ця система соціального кредитування вивести Китай на шлях тоталітаризму. Однак, незважаючи на це, розвиток цієї системи продовжується, а китайські інвестиції у світову економіку постійно зростають.

Уряд Китаю активно працює над довгостроковим планом, щоб використати своє багатство і промислові ноу-хау для очолення нової глобалізації 2.0, яка відмовлятиметься від правил західних інституцій. Ціль полягає в тому, щоб перетворити глобальний економічний порядок, залучаючи країни та компанії до китайської орбіти. Про це повідомляє "The New York Times", посилаючись на директора Центру міжнародного співробітництва Національної комісії розвитку і реформ Као Венліан.

У своїй стратегії Китай будує мости, аеропорти, залізниці та електростанції, закріплюючи свої можливості впливу через інфраструктурні проекти. Ці

ініціативи охопили не лише країни Азії, але й Україну. Наприклад, китайці допомагають у модернізації Укртелекому, не дивлячись на новини про несплату компанією та її акціонером мільярдних боргів за облігаціями. China Development Bank і Huawei, які є головними інвесторами, мають право отримати будівлі компанії та обладнання в разі непогашення боргу через заставу за мільярдні кредити. Укртелеком надав китайському банку права на вимогу за певними банківськими рахунками. Таким чином, майно однієї з провідних компаній українського ринку телекомунікаційних послуг, яка забезпечує функціонування інформаційно-телекомунікаційних систем критичних об'єктів інфраструктури країни, може опинитися у власності китайських компаній, що контролюються владою Китаю.

2.3. Агентивний фактор національних цифрових продуктів в Україні.

Основним законом у сфері надання адміністративних послуг є Закон України «Про адміністративні послуги», у пункті першому статті 17 якого зазначено, що: «Надання адміністративних послуг в електронній формі та доступ суб'єктів звернення до інформації про адміністративні послуги з використанням мережі Інтернет забезпечуються засобами Єдиного державного веб-порталу електронних послуг, який є офіційним джерелом інформації про надання адміністративних послуг в Україні» [6].

Питання функціонування Єдиного державного веб-порталу електронних послуг (далі - Портал Дія) регулюються Положенням «Про Єдиний державний веб-портал електронних послуг», затвердженим постановою КМ України від 4 грудня 2019 року № 1137.

Відповідно до положень даного нормативно-правового акту, основними завданнями Порталу Дія є:

- надання електронних послуг (в тому числі адміністративних та інших публічних послуг);
- забезпечення через електронний кабінет користувача доступу до інформації з національних електронних інформаційних ресурсів, зокрема про користувача;
- отримання суб'єктами звернення результатів надання електронних послуг, розгляду звернень та адміністративних справ;

забезпечення користувачів інформацією про електронні та адміністративні послуги, а також про інші публічні послуги, надання яких здійснюється з використанням Порталу Дія;

- подання електронних звернень через Портал Дія та інші [7].

Також отримати електронні адміністративні послуги можливо через офіційні вебсайти ЦНАПів у розділах «Реєстр послуг», де наведений вичерпний перелік адміністративних послуг, які можна отримати онлайн. Потрібно звернути увагу на те, що процес отримання електронних адміністративних послуг як за допомогою Порталу Дія, так і через веб сайти ЦНАПів відбувається за допомогою використання кваліфікованого електронного підпису (КЕП) [8, с. 268].

Питання формування законодавчих засад цифровізації та цифрового суспільства належить до відання не тільки Верховної Ради України, як органу законодавчої влади, але й до відання відповідного центрального органу виконавчої влади з точки зору формування та реалізації державної політики у сфері цифровізації, цифрового розвитку, цифрової економіки, цифрових технологій та інновацій, електронної демократії, електронного урядування тощо. В Україні це Міністерство цифрової трансформації України, яке було утворено постановою КМ України від 02 вересня 2019 р. № 829 шляхом реорганізації Державного агентства з питань електронного урядування.

Одними з основних завдань Міністерства цифрової трансформації України є саме розробка та впровадження в національну політику новацій у таких сферах як: надання електронних та адміністративних послуг, розвиток цифрових навичок та цифрових прав громадян, цифровізація, цифровий розвиток, цифрова економіка, цифрові інновації та технології, електронне урядування та електронна демократія, розвиток інформаційного суспільства. Крім того, відповідно до покладених на нього завдань, Міністерство цифрових трансформацій узагальнює практику застосування законодавства з питань, які належать до його компетенції, розробляє пропозиції щодо

вдосконалення відповідних нормативно-правових актів та проекти таких актів [9].

Проте варто погодитися з тезою про те, що кожне нововведення в структуру функціонування суспільних відносин має як позитивні аспекти, так і негативні. Не стала виключенням з цього правила і цифровізація адміністративних послуг в Україні, яка поряд зі сприятливою для громадян стороною, має певні недоліки не лише у правовому регулюванні, а й у процесі функціонування загалом.

Головною метою цифровізації адміністративних послуг є полегшення комунікації з органами державної влади та місцевого самоврядування. Проте у процесі реалізації постала проблема так званої «цифрової нерівності». Користування інтернет-технологіями передбачає наявність у особи відповідних знань та навичок, проте внаслідок низького рівня цифрової грамотності не всі громадяни можуть користуватися новим способом отримання адміністративних послуг.

За даними Міністерства цифрової трансформації України рівень цифрової грамотності серед українців становить нижче середнього [10, с. 216]. У цей же час спостерігається яскраво виражений цифровий розрив між селом та містом – близько 35–40%. Наразі у стані цифрової нерівності перебувають близько 8 мільйонів українців [11, с. 23].

На нашу думку, такі проблеми як цифрова нерівність та цифровий розрив – є тими бар'єрами, які необхідно подолати, щоб продовжити шлях до цивілізованої цифровізації. Ще однією актуальною проблемою у сфері цифровізації надання адміністративних послуг є відсутність налагодженої взаємодії державних систем. Наслідком цього є неможливість спрощення процесу надання такого виду послуг. Законом України «Про адміністративні послуги» передбачена заборона вимагати від осіб, що звернулися за отриманням послуги, інформацію або дані, які містяться в інших органах влади [6].

Через відсутність взаємодії, користувачі послуг зустрічаються із проблемою, яку цифровізація повинна була подолати, а саме – так звана «тяганина» з документами. Крім того, не зникла проблема відсутності надійних засобів захисту для безпечного обміну ідентифікаційними даними фізичних та юридичних осіб в інформаційних системах органів державної влади. З ростом популярності надання адміністративних послуг через мережу Інтернет зростає рівень використання технічно несумісних механізмів, алгоритмів і протоколів електронної ідентифікації та ідентифікації в реєстраційних системах та системах доступу до інформаційних систем [4, с. 117].

На даному етапі впровадження цифровізації адміністративних послуг в нашій державі супроводжується також такою проблемою, як обмеженість процедури отримання певних послуг в електронному вигляді лише початковою її стадією.

І. Тищенко зазначає, що такі процеси як подання електронних документів, моніторинг процесу отримання послуги не доступні деяким користувачам. Так, наприклад, багато ЦНАПів наразі не надають можливості особам отримати електронні адміністративні послуги належного рівня. Вони лише публікують загальну інформацію про послугу, а також розміщують електронні форми та заяви [12, с. 126].

Взагалі саме функціонування WEB-сторінок ЦНАПів викликає досить багато запитань. Відповідно до даних моніторингу, що був проведений Міністерством розвитку економіки, торгівлі та сільського господарства України (далі - Мінекономіки), можна констатувати факт відсутності в деяких ЦНАПів і власного WEB-сайту, і своєї сторінки на сайті органу місцевого самоврядування. Внаслідок чого користувачі взагалі втрачають можливість отримати будь-яку послугу в електронному режимі.

Цифровізація адміністративних послуг, повинна у повному обсязі забезпечити користувачів безпечними сервісами, метою яких буде надання доступу до детальної інформації про послугу, можливість заповнювати та

завантажувати необхідні для отримання послуги зразки та форми документів, механізмом інформування користувача про стан розгляду, а також здатністю онлайн-оплати послуги.

На даний момент, такий механізм в Україні працює недосконало, що викликає певні труднощі під час отримання адміністративних послуг за допомогою сучасних технологій. На фоні ще більш активної консолідації інтернет-технологій та сучасного суспільства, набуває ще більшої актуальності вже відома проблема – проблема кіберзлочинності, яка загрожує персональним даним користувачів послуг, в умовах збільшення кількості інформаційних систем. Крім зазначених вище проблем та аспектів, правовий аспект цифровізації адміністративних послуг також має недоліки, які потребують вирішення. Дані проблеми можна виявити на окремих етапах отримання послуги. Так, наприклад, на першому етапі надання адміністративної послуги – подачі заяви - ми зустрічаємося з проблемою відсутності визначення питання легітимізації електронної форми заяви, що заповнюється безпосередньо на WEB-сторінках. На сьогодні існує два варіанти заповнення електронної форми заяви – завантаження заяви, її заповнення та подальша передача із застосуванням електронного цифрового підпису (дана процедура законодавчо визначена), а також за допомогою заповнення екранної форми заяви безпосередньо на WEB-сторінці. І саме другий варіант потребує правового врегулювання. Наразі відсутній механізм, який повинен врегульовувати питання підпису або його аналогу саме екранної форми, що є необхідним для підтвердження волевиявлення сторін, внаслідок чого відсутня можливість ідентифікації суб'єкта отримання послуги [13, с. 3].

Наступна, проте не менш важлива та актуальна на сьогодні правова проблема цифровізації адміністративних послуг пов'язана з таким етапом надання електронної адміністративної послуги як робота суб'єкта надання послуги над отриманими заявами та документами. На цій стадії активно використовується електронна міжвідомча функціональна взаємодія при

опрацюванні отриманих заяв та документів. З одного боку Законом України «Про адміністративні послуги» визначено обов'язок суб'єктів надання адміністративних послуг, які володіють певною необхідною для надання цього виду послуг інформацією, забезпечувати доступ до такої інформації та її захист.

Проте проблема, на яку необхідно звернути увагу полягає в тому, що в законодавстві наразі невизначеними залишаються положення щодо організації електронної взаємодії учасників надання адміністративних послуг, а саме невизначеними є їхні права та обов'язки: по-перше, не визначена можливість передачі запиту на інформацію від одного органу до іншого та отримання відповіді за допомогою засобів телекомунікацій, що впливає на весь процес переведення надання адміністративних послуг в електронну форму; по-друге, законом не передбачений вичерпний перелік суб'єктів надання адміністративних послуг, які можуть нести відповідальність за неналежне забезпечення суб'єкта звернення відомостями, що запрошуються в запиті [13, с. 4].

Наслідком вказаної проблеми є неможливість на даному етапі отримання адміністративної послуги визначити суб'єкта, який відповідальний за ненадання або неналежне надання послуги. Також можна констатувати факт наявності недоліків у регламентації самого процесу переходу безпосередньо до електронної взаємодії між учасниками процесу.

Вдосконалення у правовому регулюванні потребують і певні технічні моменти процесу надання адміністративної послуги за допомогою інтернет-технологій. До таких моментів належить: потреба в чіткій регламентації часу відправлення та отримання інформаційних матеріалів, які будуть вагомим юридичним фактом для звернення чи оскарження до суду; створення можливостей надсилання документів за допомогою всіх сервісів «Електронний кабінет»; регламентація часу відправлення та одержання інформаційних матеріалів, а саме електронних послуг, супутніх документів, що будуть достатнім юридичним фактом при зверненні до суду чи

оскарженні; створення можливостей для направлення документів за допомогою усіх сервісів «Електронний кабінет» [8, с. 267].

Підсумовуючи, слід зазначити, що цифровізація адміністративних послуг в Україні є процесом, який покликаний спростити процедуру надання адміністративних послуг, використовуючи при цьому інтернет-технології. Даний процес має переважно позитивний ефект на суспільні відносини. Проте, досліджуючи процедуру отримання таких послуг та нормативно-правову базу, а саме профільні закони у даній сфері та акти Кабінету Міністрів України, було виявлено ряд недоліків, які негативно впливають на цифровізацію загалом. З метою вирішення зазначених проблем, пропонуємо ряд рекомендацій, які стосуються як безпосередньо процедури надання та отримання адміністративних послуг за допомогою інтернет-технологій, так і правових аспектів їх врегулювання. Практична реалізація запропонованого матиме позитивний вплив на процедуру цифровізації.

До першої групи рекомендацій (неправового характеру) можна віднести:

- забезпечення доступу до швидкісного інтернету по всій території України, а також проведення кампаній з підвищення цифрової грамотності громадян (ці заходи покликані подолати «цифрову нерівність» серед українського населення);
- створення єдиної та, найголовніше, ефективної системи міжвідомчого документообігу з метою вільного доступу до електронних документів суб'єктів надання адміністративних послуг;
- покращення технічної оснащеності ЦНАПів та забезпечення функціонування офіційних WEB-сторінок, через які в громадян буде доступ до отримання послуг в електронному режимі.

До другої групи рекомендацій (правового характеру) можна віднести: затвердження на законодавчому рівні ефективного алгоритму взаємодії між суб'єктами надання адміністративних послуг в режимі онлайн; затвердження особливої форми електронного підпису або його аналогу для заяв та

документів екранної форми, які у процесі отримання послуги заповнюються безпосередньо на WEB-сторінці.

Резюмуючи, слід зазначити, що Україна має всі можливості для побудови ефективної системи цифровізованих адміністративних послуг. У нашій країні зроблено вже багато кроків, покликаних на ефективне функціонування даного процесу. Проте, як і з будь-яким новим процесом, який імплементується в суспільні відносини, виникають певні проблеми в його реалізації. І лише за умови системного підходу до вирішення цих проблем, вдасться забезпечити якісний рівень функціонування системи електронних адміністративних послуг, як одного з важливих чинників розвитку демократії в країні та підвищення якості життя громадян нашої держави.

Однією з головних проблем цифровізації політики в Україні є недостатній розвиток технічної та інфраструктурної бази. Багато сільських та віддалених регіонів країни досі не мають доступу до ширококутового інтернету, що значно обмежує можливості місцевих жителів у доступі до електронних послуг та інформації. У таких умовах громадяни не можуть користуватися електронними урядовими сервісами, брати участь в онлайн-консультаціях та обговореннях, або отримувати важливу інформацію про діяльність державних органів. Крім цього, навіть у тих регіонах, де інтернет-зв'язок є, його якість часто залишає бажати кращого. Недостатня пропускну здатність мереж, низька якість зв'язку та часті перебої в роботі інтернету створюють значні труднощі для ефективного використання цифрових технологій. Наприклад, відеоконференції, які є важливим інструментом для дистанційної роботи та навчання, можуть бути перервані через поганий зв'язок, що ускладнює комунікацію та координацію дій між державними органами та громадянами [5, с. 16].

Додатково до проблем з інтернет-зв'язком, державні органи часто використовують застаріле обладнання та програмне забезпечення. Багато комп'ютерів та серверів, які використовуються в урядових установах, не

відповідають сучасним вимогам безпеки та продуктивності. Це означає, що системи можуть бути вразливими до кібератак, а їхня продуктивність може бути недостатньою для обробки великих обсягів даних, що зростають у процесі цифровізації. Застарілі системи також ускладнюють інтеграцію новітніх технологій, таких як блокчейн або штучний інтелект, які можуть значно покращити ефективність та прозорість державного управління. Наприклад, впровадження електронного голосування або автоматизованих систем аналізу даних вимагає сучасного програмного забезпечення та обладнання, яке може забезпечити безпеку і швидкість обробки інформації. Крім того, відсутність належного фінансування та підтримки з боку держави призводить до того, що модернізація технічної інфраструктури відбувається повільно. Державні органи часто не мають достатніх коштів для оновлення своїх систем та впровадження нових технологій, що знижує їхню здатність ефективно працювати в умовах цифрової трансформації [7, с. 458].

Законодавча та нормативна база, що регулює цифровізацію політики в Україні, часто відстає від швидких темпів розвитку технологій. Це призводить до того, що законодавчі акти можуть бути неузгодженими або застарілими, створюючи правову невизначеність, яка гальмує впровадження нових цифрових рішень. Наприклад, відсутність чітких регуляцій щодо електронного голосування ускладнює реалізацію таких проектів на практиці. Відсутність законодавчого визначення електронного голосування та процедур, які забезпечують його безпеку та конфіденційність, робить цей процес вразливим до маніпуляцій та підриву довіри громадян. Процес прийняття нових законів може бути тривалим і супроводжуватися значними бюрократичними перешкодами. Це означає, що навіть необхідні законодавчі зміни можуть затримуватися на роки, не встигаючи за технологічними нововведеннями. Бюрократичні процеси, відсутність координації між різними державними органами та політична нестабільність можуть уповільнити або повністю зупинити процес цифровізації [11, с. 127].

Наприклад, захист персональних даних є ще однією важливою складовою законодавчої бази. Закон України «Про захист персональних даних» був прийнятий у 2010 році, але деякі його положення потребують оновлення, щоб відповідати сучасним європейським стандартам. Важливою проблемою є те, що не всі державні органи та приватні компанії в Україні дотримуються норм законодавства щодо захисту персональних даних. Недостатня імплементація цього закону призводить до численних випадків витоку та несанкціонованого використання персональних даних громадян, що може мати серйозні наслідки для їхньої приватності. Громадяни втрачають довіру до цифрових сервісів, що перешкоджає їх активному використанню.

Наприклад, Закон України «Про доступ до публічної інформації» гарантує право громадян на доступ до інформації, що володіє суспільним інтересом. Проте, на практиці доступ до публічної інформації може бути ускладнений через бюрократичні перешкоди, відсутність чітких процедур та неготовність державних органів надавати інформацію у відкритий доступ. Наприклад, громадяни часто стикаються з відмовами або затримками в отриманні необхідної інформації, що ускладнює їх участь у політичному житті та прийняття обґрунтованих рішень щодо політичних питань. Державні органи можуть не мати відповідних ресурсів або бажання для забезпечення відкритого доступу до інформації, що створює додаткові бар'єри для громадського контролю та прозорості.

Питання безпеки та конфіденційності є одними з найважливіших аспектів цифровізації політики, оскільки вони безпосередньо впливають на довіру громадян до електронних послуг і державних ініціатив. У цифровому середовищі, де велика кількість інформації передається та зберігається в електронному вигляді, кіберзагрози стають все більш актуальними. Україна неодноразово стикалася з масштабними кібератаками, які мали серйозні наслідки як для державних установ, так і для приватних компаній. Зокрема, відомі кібератаки, такі як Petya та NotPetya, паралізували роботу багатьох організацій, знищували важливі дані та викликали значні економічні збитки.

Такі інциденти демонструють вразливість цифрових систем і необхідність їх належного захисту [12, с. 42].

Однією з головних проблем є недостатній рівень кібербезпеки. Багато державних установ не мають сучасних засобів захисту від кіберзагроз. Недостатньо розвинені механізми виявлення та реагування на інциденти, а також системи захисту даних, що створює сприятливе середовище для зловмисників. Відсутність регулярного аудиту безпеки та оновлень програмного забезпечення підвищує ризики витоку конфіденційної інформації та маніпуляцій з боку кіберзлочинців. Однією з найпоширеніших кіберзагроз є фішинг – спроби отримати конфіденційну інформацію шляхом обману користувачів. Це може бути здійснено через підроблені електронні листи або веб-сайти, які імітують справжні ресурси державних органів або відомих компаній [15, с. 161]. Люди, не усвідомлюючи небезпеки, можуть надати свої особисті дані, які потім використовуються зловмисниками для шахрайства. Шкідливе програмне забезпечення, яке включає віруси, троянські програми та інші види зловмисного ПЗ, також представляє значну загрозу для безпеки інформації. Таке програмне забезпечення може непомітно проникати в системи, викрадати або знищувати дані, змінювати налаштування систем та виконувати інші шкідливі дії [20]. Це може призводити до порушення роботи важливих державних служб та втрати критично важливої інформації. Конфіденційність даних також залишається важливою проблемою. В умовах цифровізації велика кількість персональних даних громадян зберігається та обробляється в електронних системах. Витоки таких даних можуть мати серйозні наслідки для приватності та безпеки громадян. Недостатньо ефективні механізми захисту персональних даних можуть призводити до їх несанкціонованого використання або продажу на чорному ринку [23].

Цифровізація політики стикається також із соціальними та культурними викликами. В Україні все ще існують значні розбіжності у рівні доступу до цифрових технологій між різними соціальними групами. Люди похилого віку, громадяни з низьким рівнем доходу або мешканці віддалених районів часто

мають обмежений доступ до Інтернету та комп'ютерної техніки, що перешкоджає їх участі в електронних політичних процесах. Крім того, культурні стереотипи та недовіра до нових технологій можуть стримувати їх широке впровадження. Недостатня обізнаність громадян про можливості цифрових інструментів у політиці також є значною перешкодою для ефективної цифровізації [26, с. 79].

Останньою, але не менш важливою проблемою є рівень цифрової грамотності населення. Багато громадян не мають достатніх навичок для ефективного використання цифрових технологій. Відсутність базових знань про комп'ютери, Інтернет та електронні послуги обмежує можливості для участі у цифрових політичних процесах. Програми навчання та підвищення цифрової грамотності, які проводяться урядом та неурядовими організаціями, часто є недостатніми або малоефективними. Це потребує більшої уваги та інвестицій у розвиток освітніх програм, спрямованих на підвищення цифрової компетентності громадян [34, с. 7].

Цифровізація політики в Україні має значний потенціал для покращення ефективності державного управління, підвищення прозорості та залучення громадян до політичних процесів. Однак для досягнення цих цілей необхідно вирішити ряд важливих завдань, пов'язаних з розвитком інфраструктури та технологій, удосконаленням законодавчої бази, підвищенням рівня цифрової грамотності населення, впровадженням міжнародного досвіду та новітніх технологій. Розвиток інфраструктури та технологій є одним з ключових напрямків цифровізації політики. Для забезпечення доступу всіх громадян до електронних послуг необхідно інвестувати в розвиток ширококутового інтернету, особливо у віддалених та сільських регіонах. Підключення до високошвидкісного інтернету має стати пріоритетом, оскільки це дозволить жителям цих регіонів користуватися електронними урядовими послугами, брати участь у дистанційних освітніх програмах та економічних активностях. Крім того, державні установи повинні оновити своє технічне обладнання та

програмне забезпечення, щоб забезпечити ефективну роботу цифрових систем та захист даних.

Удосконалення законодавчої бази є ще одним важливим аспектом. Сучасне законодавство повинно відповідати швидкому розвитку технологій та забезпечувати правову визначеність для впровадження нових цифрових рішень. Наприклад, необхідно прийняти закони, які регулюють електронне голосування, захист персональних даних та кібербезпеку. Ці законодавчі акти мають забезпечити безпеку та конфіденційність інформації, а також визначити відповідальність за порушення в цій сфері. Швидке та ефективне прийняття таких законів сприятиме створенню сприятливих умов для цифровізації політичних процесів.

Підвищення рівня цифрової грамотності населення є критично важливим для успішної цифровізації політики. Високий рівень цифрової грамотності дозволяє громадянам ефективно користуватися електронними послугами, брати участь у політичних дискусіях онлайн та контролювати діяльність державних органів. Для цього необхідно розробити та впровадити програми навчання, які охоплюватимуть різні вікові та соціальні групи. Освітні ініціативи повинні включати як базові навички роботи з комп'ютером та Інтернетом, так і більш складні аспекти, такі як кібербезпека та використання спеціалізованих цифрових платформ.

Міжнародний досвід та його імплементація в Україні є важливим джерелом знань та передових практик. Багато країн вже мають успішний досвід цифровізації політики, і Україна може використовувати ці напрацювання для вдосконалення власних процесів. Наприклад, Естонія відома своїми досягненнями в галузі електронного урядування та електронного голосування, і їхній досвід може бути корисним для України. Важливо вивчати міжнародні моделі та адаптувати їх до національних реалій, беручи до уваги культурні та соціальні особливості країни. Це допоможе уникнути помилок та забезпечити успішну імплементацію цифрових ініціатив.

Впровадження новітніх технологій, таких як блокчейн та штучний інтелект, має великий потенціал для покращення політичних процесів в Україні. Блокчейн, наприклад, може забезпечити високий рівень прозорості та безпеки в процесах голосування, зберігання даних та укладання контрактів. Ця технологія дозволяє створювати незмінні записи, що робить неможливим фальсифікацію результатів або маніпуляцію даними. Штучний інтелект може використовуватися для аналізу великих обсягів даних, прогнозування тенденцій та автоматизації рутинних завдань, що підвищує ефективність роботи державних органів та дозволяє зосередитися на стратегічних питаннях.

Застосунок «Дія» було запущено в Україні у 2020 році з метою інтеграції основних державних послуг в одному мобільному додатку. Його розробка стала частиною ширшої стратегії цифрової трансформації країни, спрямованої на модернізацію державного управління та підвищення ефективності взаємодії громадян з державою. Основною метою застосунку «Дія» було створення єдиного цифрового простору, де громадяни могли б отримати доступ до різноманітних державних послуг без потреби відвідувати державні установи фізично. Цей підхід сприяв значному скороченню часу та ресурсів, необхідних для отримання державних послуг. Застосунок дозволяє користувачам мати цифрові версії своїх документів, таких як паспорт, водійське посвідчення, технічний паспорт на автомобіль тощо. Це значно спрощує процеси ідентифікації та верифікації, що раніше вимагали наявності паперових документів [13]. Крім того, «Дія» надає можливість отримувати різноманітні адміністративні послуги онлайн. Наприклад, громадяни можуть зареєструвати бізнес, отримати необхідні довідки або інші офіційні документи без потреби відвідувати державні установи. Це забезпечує зручність і швидкість обробки запитів, що особливо важливо в умовах сучасного швидкоплинного світу. Інформаційна підтримка громадян також є важливою функцією «Дія». Застосунок забезпечує користувачів своєчасними сповіщеннями про важливі події, зміни в законодавстві, нові можливості та послуги. Це дозволяє

громадянам бути в курсі актуальних новин та швидко адаптуватися до змін, що відбуваються в державному управлінні [13].

Зручність та доступність є одними з найголовніших переваг застосунку «Дія». Він дозволяє громадянам отримувати державні послуги без необхідності особистого відвідування державних установ, що значно економить час та ресурси. Це особливо важливо для тих, хто живе у віддалених регіонах, де доступ до державних установ може бути обмеженим або вимагає значних зусиль для досягнення. Прозорість процесів, забезпечена цифровізацією через «Дію», знижує ризики корупції та зловживань. Автоматизація процедур і зменшення людського фактору роблять процеси більш відкритими та підконтрольними, що підвищує довіру громадян до державних інституцій. Інклюзивність «Дії» полягає в тому, що застосунок забезпечує доступ до державних послуг для всіх верств населення, включаючи ті, що живуть у віддалених або менш розвинених регіонах. Це сприяє рівноправному доступу до послуг та інформації, що є важливим кроком до створення справедливого та рівноправного суспільства [4].

Незважаючи на значні переваги, впровадження застосунку «Дія» стикається з низкою викликів. Одним з найбільш критичних аспектів є безпека даних. У цифровому світі захист персональних даних громадян від кібератак та несанкціонованого доступу стає першочерговим завданням. Оскільки «Дія» обробляє велику кількість чутливої інформації, будь-які витоки або порушення безпеки можуть мати серйозні наслідки для користувачів. Тому впровадження найсучасніших технологій захисту даних, постійне оновлення систем безпеки та проведення аудитів є обов'язковими кроками для забезпечення надійності застосунку. Іншим значним викликом є технічна інфраструктура. Застосунок повинен забезпечувати стабільну роботу на всій території країни, включаючи регіони з обмеженим доступом до інтернету. Це потребує розвитку мережі широкосмугового інтернету, модернізації існуючих комунікаційних мереж та створення умов для стабільного підключення в сільських та віддалених районах. Відсутність доступу до інтернету може стати

бар'єром для використання «Дії» значною частиною населення, що знижує ефективність цифровізації [24].

Цифрова грамотність населення також є важливим чинником успішного впровадження «Дії». Багато громадян, особливо старшого віку або з низьким рівнем освіти, можуть не мати достатніх знань та навичок для ефективного використання цифрових послуг. Для подолання цього виклику необхідні програми з навчання та підвищення цифрової грамотності, які б забезпечили громадянам необхідні знання для використання «Дії» та інших цифрових інструментів. Це може включати як онлайн-курси, так і офлайн-тренінги та підтримку на місцевому рівні [30].

Розвиток «Дії» та подібних ініціатив може мати значний вплив на подальшу цифровізацію державного управління. Одним із перспективних напрямків розвитку є розширення функціональності застосунку. Додавання нових послуг та функцій, що покривають більший спектр потреб громадян, дозволить зробити «Дію» ще більш корисною та зручною. Наприклад, можна включити сервіси, пов'язані з охороною здоров'я, освітою, соціальним забезпеченням тощо. Це дозволить громадянам отримувати всі необхідні державні послуги в одному місці, що значно підвищить ефективність їх взаємодії з державними органами [13].

Міжнародне співробітництво також відіграє важливу роль у розвитку «Дії». Обмін досвідом та технологіями з іншими країнами дозволить покращити власні цифрові рішення та впроваджувати передові практики. Це може включати участь у міжнародних конференціях, спільні проекти з розробки нових технологій, а також обмін фахівцями та знаннями. Таке співробітництво сприятиме підвищенню рівня цифровізації та інноваційності в державному управлінні. Інтеграція з іншими системами є ще одним важливим напрямком розвитку. Сприяння інтеграції «Дії» з міжнародними цифровими платформами та системами забезпечить зручність використання послуг громадянами, які перебувають за кордоном. Наприклад, це може включати обмін даними з системами інших країн для полегшення процесів

ідентифікації, верифікації та отримання державних послуг для українців, які тимчасово чи постійно проживають за кордоном [27].

Отже, застосунок «Дія» став важливим кроком у напрямку цифровізації державного управління в Україні. Він демонструє значний потенціал у підвищенні ефективності, прозорості та доступності державних послуг для громадян. Завдяки «Дії» українці отримали можливість швидко та зручно взаємодіяти з державними органами, використовуючи свої мобільні пристрої. Це зменшує бюрократичні перепони, економить час і ресурси, а також сприяє зниженню рівня корупції. Однак впровадження застосунку «Дія» також супроводжується низкою викликів. Захист персональних даних, забезпечення стабільної технічної інфраструктури та підвищення цифрової грамотності населення є ключовими аспектами, які потребують постійної уваги та вдосконалення. Подолання цих викликів є критично важливим для успішного розвитку застосунку та його подальшої інтеграції в повсякденне життя громадян. Перспективи розвитку застосунку «Дія» є обнадійливими. Розширення функціональності, міжнародне співробітництво та інтеграція з іншими системами дозволять зробити застосунок ще більш корисним та зручним. Успішна реалізація цих напрямків сприятиме подальшій цифровізації державного управління, підвищенню якості надання державних послуг та зміцненню довіри громадян до державних інституцій.

Таким чином, «Дія» є прикладом того, як сучасні технології можуть трансформувати взаємодію між державою та громадянами, створюючи більш ефективне, прозоре та доступне державне управління. Продовження роботи над розвитком цього застосунку та подолання існуючих викликів визначатиме майбутнє цифрової держави в Україні та її здатність відповідати на виклики сучасного світу.

ВИСНОВКИ

У процесі аналізу було досліджено широкий спектр теоретичних і практичних аспектів цифровізації політики, які знайшли своє застосування у сучасному політичному ландшафті України. Визначено, що цифровізація політики впливає на усі рівні політичної діяльності, модифікує традиційні підходи і створює нові інструментарії для взаємодії влади та громадян.

Відповідно до мети і завдань дослідження були сформульовані наступні висновки:

Дослідження показало, що цифровізація політики включає застосування цифрових технологій для модернізації політичних процесів, підвищення взаємодії з громадянами та забезпечення більшої прозорості управління. Це поняття також передбачає створення цифрових платформ, що сприяють активнішій участі громадян в політиці та виборчих процесах.

Цифрові технології сприяють впровадженню інновацій у політичні стратегії, ефективнішому збору та аналізу даних, що забезпечує поліпшення прийняття рішень. Вони також допомагають політичним партіям та урядам здійснювати більш цільовий вплив на виборців через персоналізовані маркетингові кампанії та соціальні медіа.

Основними проблемами є недостатнє розуміння серед політиків важливості цифрових ініціатив, відсутність єдиних стандартів безпеки та приватності даних, а також обмежений доступ до цифрових сервісів у віддалених регіонах. Проте, перспективи розвитку цифровізації включають поліпшення участі громадськості в управлінні та підвищення прозорості державних структур.

Цифрові інструменти визнані ефективними у залученні громадян та зборі зворотного зв'язку, особливо через застосунки і соціальні мережі. Водночас, потрібно враховувати ризики зловживань та маніпуляцій, що можуть негативно вплинути на довіру до політичних інституцій.

Розробка національної стратегії цифровізації політики, що включатиме чіткі цілі та механізми впровадження. Необхідно також забезпечити навчання та підвищення обізнаності серед усіх заінтересованих сторін, а також встановлення суворих правил забезпечення безпеки та приватності даних.

Таким чином, цифровізація політики відкриває нові можливості для розвитку демократичних процесів, покращення взаємодії між владою та громадськістю, а також підвищення рівня прозорості та підзвітності державних інститутів. Водночас, успішна реалізація цього процесу вимагає комплексного підходу, що включає розвиток технологічної інфраструктури, вдосконалення законодавчої бази та підвищення цифрової грамотності населення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О. А., Попова І. М. Правові проблеми дистанційного надання адміністративних послуг. Університетські наукові записки. 2011. № 2. С. 242-247.
2. Венедіктова І. В. Юридична природа публічних послуг. Вісник Харківського національного університету. 2009. № 1 (5). С. 89-91.
3. Вінник О. М. Проблеми цифровізації: правовий аспект. Реформування правової системи в контексті євроінтеграційних процесів. Матеріали IV міжнародної науково-практичної конференції. 2020. С. 215-221.
4. Года М. Дії 3 роки: як застосунок зробив Україну найзручнішою у світі державою у сфері послуг. URL: https://24tv.ua/tech/chogo-diya-dosyagla-za-tri-roki-roboti-yak-vona-stala-mizhnarodno_n2250515 (дата звернення: 25.05.2024).
5. Дібікова Ю. С. Цифровізація політичного простору в Україні: проблеми та тенденції. Сучасне суспільство: політичні науки, соціологічні науки, культурологічні науки. 2023. № 2(23). С. 15-24.
6. Єгорова-Луценко Т. П. Цифровізація у сфері надання адміністративних послуг. Цифрові трансформації України 2020: виклики та реалії: зб. наук. пр. НДІ ПЗІР НАПрН України № 1 за матеріалами круглого столу, 18 березня 2020 р. Харків: НДІ ПЗІР НАПрН України, 2020. С. 53-62.
7. Єрмоленко О. О., Смальскис В. Напрями цифровізації держави та наслідки для суспільства. 2021. С. 456-460.
8. Ковальова Т. В., Гунбіна О. В. Правові проблеми надання адміністративних послуг з використанням інтернет-технологій. Наукові перспективи. Серія «Право». 2021. № 9 (15). С. 260-271.
9. Кравчук І. М. Правове регулювання надання адміністративних послуг при використанні інтернет-технологій. Правова інформатика. 2021. URL: <https://ela.kpi.ua/bitstream/123456789/15909/1/%D0%9F%D1>

%80%D0%B0%D0%B2%D0%BE%D0%B2%D0%B5%20%D1%80%D0%B5%D0%B3%D1%83%D0%BB%20
%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%20%D0%BF%D0%BE%D1%81%D0%BB%D1%83%D0%B3.pdf.

10. Крижанівська В. Цифровізація політичної участі: загрози та перспективи. Грані. 2021. Том 24. № 9. С. 82–90. DOI: 10.15421/172193

11. Стеблина Н. О. Складові цифровізації політики: цифровий форум, цифровий капітал та структура цифрових можливостей. Політикус. 2020. Вип. 5. С. 126 – 132.

12. Кузьменко О. В., Кропивна К. О. Перспективи запровадження та розвитку цифровізації в інноваційному суспільстві в Україні. Київський часопис права. 2021. № 1. С. 39-45.

13. Мінцифри запустило портал державних послуг «Дія». URL: <https://www.kmu.gov.ua/news/mincifri-zapustilo-portal-derzhavnih-poslug-diya> (дата звернення: 25.05.2024).

14. Мохова Ю. Л. Оцінка діяльності центрів надання адміністративних послуг в умовах цифровізації України. Публічне управління та митне адміністрування. 2021. № 2 (29). С. 22 – 28.

15. Панасюк В. М. Інформатизація та цифровізація: тенденції та напрями розвитку в Україні. Інтелект XXI. 2020. № 1. С. 160-165.

16. Петренко Н. О., Машковська Л. О. Цифровізація державних адміністративних послуг в Україні: нормативно-правові аспекти. Розбудова держави і права: питання теорії та конституційної практики. 2020. № 2. С. 112-119.

17. Питання Єдиного державного веб-порталу електронних послуг та Реєстру адміністративних послуг: Постанова КМУ України від 04.12.2019 р. № 1137. URL: <https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#Text>.

18. Питання Міністерства цифрової трансформації: Постанова КМ України від 18.09.2019 р. № 856. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text>.

19. Подгорна В. Цифрові платформи та їхній вплив на політичну сферу. Проблеми політичної психології. 2021. Вип. 10 (24). С. 301–309. DOI: 10.33120/porp-Vol24-Year2021-81

20. Помаза-Пономаренко А. Л., Микитюк Ю. М. Цифровізація державної політики vs. державна політика цифровізації у сфері правового регулювання : монографія. Харків: НУЦЗУ, 2021. 200 с.

21. Про адміністративні послуги: Закон України від 06.09.2012 р. № 5203-VI. URL: <https://zakon.rada.gov.ua/laws/show/5203-17#Text>.

22. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження КМУ від 07.03.2022. Офіційний вісник України. 2018. № 16. URL: <https://zakon.rada.gov.ua/laws/show/826-2020-%D0%BF>.

23. Резнікова О.О. Національна стійкість в умовах мінливого безпекового середовища: монографія. Київ: НІСД, 2022. 532 с.

24. Рік застосунку Дія: перші у світі цифрові паспорти та більше 3,6 млн зареєстрованих користувачів. URL: <https://diia.gov.ua/news/rik-zastosunku-diya-pershi-u-sviti-cifrovi-pasporti-ta-bilshe-36-mln-zareyestrovanih-koristuvachiv>

25. Сегеда О. О. Цифрова дипломатія України як елемент нової публічної дипломатії / О. О. Сегеда // Політикус : наук. журнал. – 2020. – № 3. – С. 139–148.

26. Сиченко В.В., Пугач А.М., Мареніченко В. В. Механізми державного регулювання розвитку інформаційного суспільства. Інвестиції: практика та досвід. 2020. № 5-6. С. 76-80.

27. США підтримали ідею створення аналогів застосунку “Дія” в інших країнах. URL: <https://investory.news/ssha-pidtrimali-ideyu-stvorennya-analogiv-zastosunku-diya-v-inshix-krainax/>

28. Теремко В. Розвиток політичної системи в умовах цифровізації. Літопис Волині. Всеукраїнський науковий часопис. Чис. 28. 2023. С. 300-304.
29. Тищенко І. О. Адміністративні процедури надання електронних публічних послуг публічною адміністрацією в Україні. Форум права. Юридичний форум. 2017. № 2. С. 124-129.
30. У застосунку «Дія» стали доступні документи про освіту – Федоров. URL: <https://www.radiosvoboda.org/a/news-dokumenty-pro-osvitu-diya/32872952.html>
31. Хаустова М. Державна політика в умовах цифровізації суспільства: міжнародний досвід реалізації програм та стратегій цифровізації. Аналітично-порівняльне правознавство : електронне наукове видання. 2022. № 2. С. 209–216. DOI: 10.24144/2788-6018.2022.02.40
32. Шманатов М. Цифрові технології як фактор впливу на політичні процеси: спроба концептуалізації. Вісник Харківського національного університету імені В.Н. Каразіна. 2021. Вип. 40. С. 29–37. DOI: 10.26565/2220-8089-2021-40-04
33. Щодо трансформації політичної системи в контексті європейської інтеграції: аналітична записка Національного інституту стратегічних досліджень / Ф. Вауліна та ін. Київ : НІСВ, 2014. URL: <https://niss.gov.ua/doslidzhennya/politika/schodo-transformacii-politichnoi-sistemi-v-konteksti-evropeyskoi-integracii>
34. Яненко І. Г. Чинники і шляхи розвитку цифровізації в Україні. Економіка України. 2022. № 3. С. 4-22.
35. Amazon. URL: <https://www.aboutamazon.com/>
36. Atlantic Council. Early lessons from the Russia-Ukraine war as a space conflict. URL: <https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/early-lessons-from-the-russia-ukraine-war-as-a-space-conflict/>
37. A parallel terrain: Public-private defense of the Ukrainian information environment. URL: <https://www.atlanticcouncil.org/in-depth-research->

[reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/](#)

38. A year of Russian hybrid warfare in Ukraine. URL: https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

39. Belfer Center for Science and International Affairs. (2022). Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose? URL: <https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose>

40. Burgess S. Russian 'smash-and-grab' social media operation on Facebook and Instagram attempting to influence Ukraine war - Meta report. URL: <https://news.sky.com/story/russian-smash-and-grab-social-media-operation-on-facebook-and-instagram-attempting-to-influence-ukraine-war-meta-report-12817721>

41. BBC News. Mariupol: Russia declares complete victory at Azovstal plant. URL: <https://www.bbc.com/news/world-europe-61529877> (дата звернення: 25.05.2024).

42. BBC. Elon Musk woos world leaders, courting controversy. <https://www.bbc.com/news/world-us-canada-66777096>

43. Bloomberg. Musk Told Pentagon He Spoke to Putin Directly, New Yorker Says. URL: <https://www.bloomberg.com/news/articles/2023-08-21/musk-told-pentagon-staff-he-spoke-to-putin-before-starlink-call>

44. CNBC. Musk's proposal for China-Taiwan relations gets slammed: Our freedom is 'not for sale'. URL: <https://www.cnbc.com/2022/10/10/elon-musk-wades-in-to-debate-over-taiwan-china-relations.html>

45. Defense News. SpaceX shut down a Russian electromagnetic warfare attack in Ukraine last month. URL: <https://www.defensenews.com/air/2022/04/20/spacex-shut-down-a-russian->

[electromagnetic-warfare-attack-in-ukraine-last-month-and-the-pentagon-is-taking-notes/](#)

46. Defending Ukraine: Early Lessons from the Cyber War. URL: <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>

47. Digital technology and the war in Ukraine. URL: <https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/>

48. Dwoskin E., Zakrzewski C.. “Facebook and TikTok ban Russian state media in Europe.” The Washington Post. URL: <https://www.washingtonpost.com/technology/2022/02/28/facebook-ukraine-russiandisinformation/>.

49. Elon Musk Without Masks. URL: <https://www.ukrainer.net/musk-without-masks/>

50. Google, Meta and Amazon will benefit from the Ukraine war, ad guru Martin Sorrell says. URL: <https://www.cnbc.com/2022/05/23/google-meta-amazon-to-benefit-from-ukraine-war-martin-sorrell-says.html>

51. How Amazon is assisting in Ukraine. URL: <https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine>
(дата звернення: 25.05.2024).

52. How Amazon put Ukraine’s ‘government in a box’ — and saved its economy from Russia. URL: <https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data>

53. How Facebook pages exploit Russia’s war in Ukraine with false videos. URL: <https://www.poynter.org/fact-checking/2022/how-facebook-pages-exploit-russias-war-in-ukraine-with-false-videos/>

54. Microsoft Threat Report: How Russia’s War on Ukraine Is Impacting the Global Cybersecurity Community. URL: <https://www.darkreading.com/threat-intelligence/microsoft-threat-report-how-russia-s-war-on-ukraine-is-impacting-the-global-cybersecurity-community>

55. Ministry of Digital Transformation: Amazon Web Services supports Ukraine with USD 75 million for cloud technologies to help the digital state and economy work stably. URL: <https://www.kmu.gov.ua/en/news/amazon-web-services-nadaye-ukrayini-pidtrimki-na-75-mln-dolariv-na-hmarni-tehnologiyi-yaki-dopomagayut-stabilno-pracyuvati-cifrovij-derzhavi-ta-ekonomici>

56. Oleksiy Honcharuk: National Digital Literacy Platform "Diia: Digital Education" will be launched on January 21. URL: <https://www.kmu.gov.ua/en/news/oleksij-goncharuk-nacionalna-osvitnya-platforma-z-cifrovoyi-gramotnosti-diya-cifrova-osvita-startuye-vzhe-21-sichnya>

57. Politico. UkraineX: How Elon Musk's space satellites changed the war on the ground. URL: <https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039>

58. Propaganda and Misinformation on Facebook and Twitter during the Russian Invasion of Ukraine. URL: <https://dl.acm.org/doi/fullHtml/10.1145/3578503.3583597>

59. Russian threat actors dig in, prepare to seize on war fatigue. URL: <https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/russian-threat-actors-dig-in-prepare-to-seize-on-war-fatigue>

60. Russian influence and cyber operations adapt for long haul and exploit war fatigue. URL: <https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac/>

61. Social Media as a Propaganda Tool in the Russia-Ukraine Conflict. URL: <https://www.thecaireview.com/essays/social-media-as-a-propaganda-tool-in-the-russia-ukraine-conflict/>

62. Shannon B. Facebook takes down Russian network impersonating European news outlets. URL: <https://www.npr.org/2022/09/27/1125217316/facebook-takes-down-russian-network-impersonating-european-news-outlets> (дата звернення: 25.05.2024).

63. Shamsi Z. U. H. Efficacy of Social Media in Wars and Conflicts: Brief Review of Russia-Ukraine War. CARC Research in Social Sciences. 2023. № 2(4). P. 202-207.

64. Stupp C. Ukraine Has Begun Moving Sensitive Data Outside Its Borders. URL: <https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002>

65. Schroeder E., Dack S. A parallel terrain: Public-private defense of the Ukrainian information environment. URL: <https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/>

66. The Role of Social Media and the Internet During Russia's War in Ukraine. URL: <https://medium.com/columbia-journal-of-science-tech-ethics-and-policy/the-role-of-social-media-and-the-internet-during-russias-war-in-ukraine-7ee5ef48fff2>

67. The Guardian. Ukraine says it has discovered mass burial site with 400 bodies in recaptured city – video. URL: <https://amp.theguardian.com/world/video/2022/sep/16/ukraine-discovers-mass-burial-site-with-400-bodies-in-recaptured-city-video> (дата звернення: 25.05.2024).

68. <https://www.nytimes.com/news-event/ukraine-russia>

69. Trends We're Tracking: New Ground for Amazon, Deep Impacts of Ukraine Conflict. URL: <https://www.investpmc.com/insights/commentaries/trends-we%E2%80%99re-tracking-new-ground-amazon-deep-impacts-ukraine-conflict>

70. Ukraine one year on: When tech companies go to war. URL: <https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to-war/>

71. Принципи концепції демократичної участі Й. Масуди. Реферат URL: <https://osvita.ua/vnz/reports/politolog/17126/>