DOI 10.31558/2519-2949.2026.2.8
УДК 321:004:342.7:316.77

ORCID ID: https://orcid.org/0009-0002-3439-2498
Косенко М. С., Міжнародний університет (м. Одеса)

ЦИФРОВА СУВЕРЕННІСТЬ ТА Е-ДЕМОКРАТІЯ: БАЛАНС МІЖ БЕЗПЕКОЮ ДАНИХ ТА ПРОЗОРІСТЮ ПОЛІТИЧНОГО ПРОЦЕСУ

У статті здійснено комплексний аналіз взаємозв'язку між цифровою суверенністю та електронною демократією в умовах інтенсивної цифровізації політичних процесів. Дослідження зосереджене на виявленні ключового балансу між необхідністю забезпечення кібербезпеки, захисту персональних і державних даних та збереженням прозорості й відкритості політичного процесу. Обґрунтовано, що цифрова суверенність виступає багатовимірною категорією, яка охоплює технологічний контроль над інфраструктурою, нормативне регулювання цифрового простору та політичну автономію держав у глобальному цифровому середовищі. Електронна демократія розглядається як інструмент підвищення політичної участі громадян, розвитку підзвітності влади та зміцнення довіри до інститутів управління. Проаналізовано досвід ЄС як провідної моделі «людиноцентричної цифровізації», що базується на поєднанні високих стандартів захисту даних, регулювання цифрових платформ та стратегічного розвитку штучного інтелекту. Показано, що ЄС прагне одночасно забезпечити технологічну автономію та гарантувати демократичні права громадян, однак стикається з викликами алгоритмічної непрозорості, дезінформації та залежності від глобальних технологічних корпорацій. Окрему увагу приділено механізмам протидії інформаційним загрозам і розвитку цифрових інструментів участі, включаючи електронне голосування, петиції та платформи відкритих даних. Визначено, що для України проблема балансу між безпекою та прозорістю набуває особливої актуальності в умовах війни та гібридних загроз. Підкреслено необхідність гармонізації національного законодавства з європейськими стандартами, розвитку кіберзахисту, цифрової інфраструктури та підвищення рівня цифрової довіри громадян. Зроблено висновок, що ефективна модель цифрової суверенності та е-демократії можлива лише за умови інтегрованого підходу, який поєднує правові, технологічні та інституційні механізми.

Ключові слова: *цифрова суверенність, електронна демократія, кібербезпека, захист даних, дезінформація, цифрові платформи, штучний інтелект, прозорість, цифрова стійкість, ЄС.*

Постановка проблеми. У сучасних умовах стрімкої цифровізації політичних процесів питання цифрової суверенності та електронної демократії набувають особливої актуальності. Формування цифрового простору як середовища політичної комунікації супроводжується посиленням як демократичних практик (участь громадян, прозорість, відкриті дані), так і нових ризиків, пов'язаних із безпекою даних, кіберзагрозами та маніпуляцією інформацією. Відповідно, ключовим викликом стає пошук балансу між забезпеченням захисту персональних і державних даних та підтриманням відкритості політичних процесів.

Особливої актуальності ця проблема набуває у контексті формування цифрового суверенітету держав, який передбачає здатність контролювати цифрову інфраструктуру та інформаційні потоки. Для Європейського Союзу це питання пов'язане з досягненням технологічної автономії, а для України – з необхідністю забезпечення цифрової стійкості в умовах війни. Таким чином, виникає науково-практичне завдання щодо пошуку ефективного балансу між безпекою даних і відкритістю політичного процесу.

Останні дослідження демонструють зростаючу увагу до цієї проблематики на рівні міжнародних інституцій та академічної спільноти. Зокрема, у комюніке Європейської Комісії щодо цифрового десятиліття підкреслюється необхідність поєднання технологічного розвитку із захистом демократичних цінностей та прав людини [12]. У звіті ENISA наголошується на зростанні складності кіберзагроз, які дедалі частіше спрямовані на державні інститути та виборчі процеси [11]. Дослідження Європейського парламенту розкривають роль цифрових технологій у трансформації демократії, зокрема через інструменти електронної участі та цифрового врядування. Водночас у

«White Paper on Artificial Intelligence» наголошується на необхідності створення довірчого середовища для використання штучного інтелекту (ШІ), що поєднує інновації та захист прав громадян [22].

Окрему увагу ЄС приділено питанням дезінформації та інформаційного втручання. Звіт Європейської служби зовнішніх дій (EEAS) 2023 року демонструє системний характер зовнішніх інформаційних маніпуляцій, які підривають демократичні процеси [8]. Водночас Європейський інспектор із захисту даних (EDPS) підкреслює необхідність посилення захисту персональних даних у цифровому середовищі [10].

Звіт Європейської Комісії 2024 року щодо реалізації програми «Digital Decade 2030» [13] аналізує чотири ключові напрями: цифрова інфраструктура, цифрові навички населення, цифровізація бізнесу та цифровізація державних послуг. Документ розглядає цифрову суверенність як одну з ключових умов стратегічної автономії ЄС у глобальному цифровому середовищі. У документі наголошується, що ЄС прагне зменшити залежність від зовнішніх технологічних платформ і посилити власні можливості у сферах ШІ, хмарних технологій, напівпровідників, кібербезпеки та цифрової інфраструктури. Особлива увага приділяється розвитку безпечного цифрового простору, захисту персональних даних, цифрових прав громадян та стійкості критичної інфраструктури.

У звіті підкреслюється, що цифрова трансформація державного управління та розвиток електронних сервісів мають поєднуватися з гарантуванням прозорості політичного процесу, кіберзахистом і контролем над використанням даних. ЄС розглядає цифрову суверенність як інструмент забезпечення демократичної стійкості, конкурентоспроможності та незалежності в умовах глобальної технологічної конкуренції.

У сучасному науковому дискурсі проблема цифрової суверенності ЄС розглядається як багатовекторний баланс, де безпека даних виступає фундаментом, а прозорість – запобіжником від авторитаризму. Зокрема, Л. Флориді, К. Кет та М. Таддео обґрунтовують концепцію «інформаційного суверенітету», підкреслюючи необхідність етичного регулювання цифрового простору [14]/ М. Чернявський стверджує, що європейська модель суверенітету відрізняється від китайської чи американської саме через пріоритет захисту прав людини над державним контролем або комерційною вигодою [9]. Водночас європейські аналітики наголошують, що прозорість алгоритмів у системі е-демократії є критичною для подолання «дефіциту довіри» виборців.

Вітчизняні дослідження цифрової суверенності та е-демократії зосереджені на проблемі поєднання відкритості влади, цифрової участі громадян і захисту даних. П. Петров підкреслює значення е-демократії для політичної участі та необхідність інформаційної безпеки [5], В. Шебанов розглядає цифрову демократію як складову цифрового врядування та трансформації взаємодії держави й суспільства [7]. Ю. Крилова акцентує увагу на балансі між прозорістю влади та захистом персональних даних [4], І. Симисенко аналізує е-демократію в умовах війни та ризики цифрової залежності від зовнішніх платформ [6], О. Антонова та С. Шаталов наголошують на ролі цифрової держави у розвитку громадянського суспільства та потребі кіберзахисту [1], Е. Войнова досліджує вплив цифрових технологій на довіру, права людини та політичну комунікацію [2], Р. Кірін акцентує увагу на необхідності вдосконалення законодавства та системи захисту даних у сфері е-урядування [3].

Попри значний масив досліджень, низка питань залишається недостатньо розробленою. Зокрема, відсутній цілісний підхід до інтеграції політик цифрової безпеки та електронної демократії; недостатньо досліджено механізми узгодження прозорості алгоритмічних систем із вимогами конфіденційності; потребує подальшого аналізу вплив цифрового суверенітету на реальні практики політичної участі громадян.

Метою статті є комплексний аналіз взаємозв'язку між цифровою суверенністю та електронною демократією, визначення ключових ризиків і проблем, а також обґрунтування механізмів досягнення балансу між безпекою даних і прозорістю політичного процесу на прикладі ЄС та України.

Виклад основного матеріалу дослідження. Цифрова суверенність у сучасному політичному дискурсі розглядається як здатність держави або наднаціонального утворення контролювати власну цифрову інфраструктуру, дані та технологічні процеси. Цифровий суверенітет є багатовимірним поняттям, що включає технічний, політичний та правовий аспекти. У технічному вимірі він означає контроль над інфраструктурою та даними, у політичному – здатність держави формувати правила цифрового простору, у правовому – створення нормативної бази для регулювання цифрових процесів.

Наукові дослідження [1; 3; 5; 7; 14] підкреслюють, що цифровий суверенітет дедалі більше стає

інструментом геополітичної конкуренції, тоді як е-демократія є механізмом легітимації влади.

Е-демократія, у свою чергу, передбачає використання цифрових технологій для забезпечення участі громадян у прийнятті політичних рішень. Її ефективність залежить від рівня довіри до цифрових інститутів і забезпечення прозорості їх функціонування.

Сучасні інструменти електронної демократії в ЄС та Україні еволюціонують від простих засобів комунікації до складних екосистем безпосереднього впливу на державне управління. На базовому рівні інформування та прозорість (e-informing) забезпечується через портали відкритих даних (в Україні – це Prozorro), електронне декларування статків посадовців та публічні реєстри власності й бізнесу, що гарантує прозорість і моніторинг діяльності влади. Більш глибоку взаємодію пропонують інструменти консультування та обговорення (e-consultation), зокрема механізми електронних петицій, платформи для обговорення законопроєктів та цифрові опитування (наприклад, у застосунку Дія), які дозволяють отримувати оперативний зворотний зв'язок від суспільства. Найвищий ступінь залученості реалізується через інструменти активної участі та прийняття рішень (e-decision making), де громадяни безпосередньо розподіляють ресурси через бюджети участі, використовують дистанційне електронне голосування (e-voting) або ініціюють законодавчі зміни на рівні ЄС через Європейську громадянську ініціативу (ECI). Важливим компонентом підзвітності влади є інструменти контролю та взаємодії (e-accountability), серед яких електронні звернення та інтерактивні мапи проблем, де кожен може зафіксувати потребу в ремонті чи іншу комунальну проблему.

Функціонування цієї системи неможливе без надійної технологічної основи, яка у 2026 році базується на цифровій ідентифікації особи через eID (BankID, Дія.Підпис), застосуванні блокчейну для захисту результатів голосувань від маніпуляцій та використанні штучного інтелекту для аналізу великих масивів коментарів і фільтрації ботів під час публічних консультацій.

Європейський Союз демонструє одну з найбільш системних і інституційно оформлених моделей поєднання цифрової суверенності та е-демократії, яка базується на принципі «людиноцентричної цифровізації». Цей підхід передбачає, що технологічний розвиток не є самоціллю, а підпорядковується захисту прав людини, демократичним стандартам і верховенству права. Одним із найбільш показових прикладів успіху є впровадження Загального регламенту захисту даних (General Data Protection Regulation) [15], який встановлює високі стандарти захисту персональних даних, що сприяє підвищенню довіри громадян до цифрових сервісів. Цей регламент також став глобальним стандартом (так званий «Brussels effect»). Наприклад, міжнародні компанії, такі як Google та Meta, були змушені адаптувати свої політики конфіденційності до вимог GDPR, навіть поза межами ЄС. Це демонструє, що цифрова суверенність може реалізовуватися не лише через контроль інфраструктури, але й через нормативну силу. Водночас викликом стало те, що надмірна складність регулювання створює бар'єри для малих і середніх підприємств, які не мають достатніх ресурсів для забезпечення відповідності вимогам. Шляхом подолання цієї проблеми стало впровадження рекомендаційних механізмів і роз'яснень, а також розвиток інституційної підтримки бізнесу.

Подальший розвиток політики цифрової суверенності відображено у пакеті цифрових актів, зокрема Digital Services Act та Digital Markets Act. Так, Закон про цифрові послуги (Digital Services Act) [17] спрямований на підвищення прозорості діяльності онлайн-платформ. Наприклад, великі платформи зобов'язані розкривати принципи роботи алгоритмів рекомендацій та модерації контенту. Це створює передумови для більшої підзвітності цифрових акторів і зменшує ризики маніпуляцій. Однак на практиці виникає конфлікт між прозорістю та комерційною таємницею алгоритмів, а також ризик надмірної цензури. Зокрема, платформи можуть видаляти контент превентивно, щоб уникнути санкцій, що може обмежувати свободу слова. Для вирішення цього виклику ЄС розвиває механізми незалежного аудиту алгоритмів і посилює судовий контроль за рішеннями платформ.

Акт про цифрові ринки (Digital Markets Act) [16] акцентує увагу на забезпечення підзвітності технологічних компаній. Ці два акти демонструють прагнення ЄС знайти баланс між свободою вираження поглядів і необхідністю протидії незаконному контенту та дезінформації. Такий підхід безпосередньо пов'язаний із розвитком е-демократії, оскільки цифрові платформи стали ключовими каналами політичної комунікації.

Значним досягненням ЄС є також розвиток електронної демократії на національному рівні. Найбільш відомим прикладом є досвід Естонії, яка впровадила систему електронного голосування (i-Voting). Це дозволило підвищити рівень участі громадян, однак водночас актуалізувало питання кібербезпеки. Для їх вирішення використовуються криптографічні методи захисту та система цифрової ідентифікації.

Ще одним прикладом є ініціатива «European Citizens' Initiative» [19], яка дозволяє громадянам ЄС безпосередньо впливати на політичний порядок денний через цифрові інструменти збору підписів. Це підсилює прозорість і підзвітність інституцій, але водночас створює ризики маніпуляцій, зокрема через автоматизовані кампанії або дезінформацію. У відповідь ЄС впроваджує механізми верифікації підписів і цифрової ідентифікації.

У ЄС питання цифрового суверенітету тісно пов'язане з прагненням зменшити залежність від глобальних технологічних гігантів і забезпечити стратегічну автономію. Попри прагнення до технологічної автономії, більшість ключових цифрових сервісів контролюються компаніями зі США або інших країн. Це створює ризики для контролю над даними та інформаційними потоками. Як відповідь, ЄС розвиває власні ініціативи, такі як проєкт Gaia-X (європейська хмарна інфраструктура, https://gaia-x.eu), спрямований на створення альтернативи глобальним хмарним сервісам. Однак цей проєкт стикається з труднощами координації між державами-членами та конкуренцією з боку вже усталених ринкових гравців.

Стратегічний курс ЄС на зміцнення цифрового суверенітету чітко простежується у ініціативі «Digital Decade 2030» [12], яка передбачає розвиток власної цифрової інфраструктури, включаючи хмарні сервіси, напівпровідники та кібербезпекові системи. Це означає не лише економічну автономію, але й здатність контролювати критично важливі дані та технології. Водночас така політика сприяє підвищенню довіри громадян до цифрових інститутів, що є необхідною умовою ефективного функціонування е-демократії.

Важливою складовою досвіду ЄС є також системна протидія дезінформації та зовнішньому втручанню. Цифровий простір ЄС характеризується зростанням ризиків. Серед них ключовими є кіберзагрози, дезінформація, алгоритмічна непрозорість і технологічна залежність. Згідно зі звітом Європейського агентства з мережевої та інформаційної безпеки (European Union Agency for Network and Information Security, ENISA), сучасний цифровий простір характеризується зростанням складних кіберзагроз, включаючи атаки на державні інституції, критичну інфраструктуру та виборчі процеси [11]. Це створює серйозні виклики для забезпечення цифрової суверенності.

У сфері протидії дезінформації важливу роль відіграє Європейська служба зовнішніх справ (European External Action Service, EEAS), яка координує зусилля щодо виявлення та аналізу інформаційних операцій. Наприклад, у звітах EEAS зафіксовано численні випадки зовнішнього втручання у виборчі процеси країн ЄС. Так, звіт EEAS 2023 року [8] демонструє, що інформаційні операції все частіше поєднуються з кіберзасобами, створюючи гібридні загрози. У таких умовах забезпечення прозорості політичного процесу стає складнішим, оскільки відкритість інформації може бути використана для маніпуляцій. Таким чином, цифровий простір стає полем гібридних конфліктів, де поєднуються кібер- та інформаційні інструменти.

У відповідь на загрози в ЄС було створено системи раннього попередження та співпраці між державами-членами. Водночас викликом залишається баланс між боротьбою з дезінформацією та захистом свободи слова. ЄС намагається вирішити цю проблему через саморегулювання платформ і розвиток медіаграмотності населення.

Окремим напрямом є розвиток регулювання штучного інтелекту. За даними Європейської парламентської дослідницької служби, у 2026 році штучний інтелект фундаментально трансформує веб, оскільки користувачі все частіше замінюють традиційні пошукові системи інструментами ШІ для отримання інформації [20]. Поява автономних агентів ШІ, здатних самостійно виконувати послідовні дії в інтернеті змінює саму природу взаємодії з цифровим середовищем. Цей зсув несе загрозу рекламній моделі доходів вебсайтів через значну втрату трафіку, що змушує видавців шукати нові економічні підходи, наприклад, через передплату або угоди з постачальниками ШІ. Водночас існує ризик поширення низькоякісного автоматизованого контенту, що може призвести до реалізації «теорії мертвого інтернету», де людська активність буде ізольована серед масових ШІ-публікацій. Концентрація влади в руках кількох великих ШІ-платформ може ще сильніше змістити баланс сил і створити умови для антиконкурентної поведінки [20].

Для зміцнення свого технологічного суверенітету та автономії Європейський Союз впроваджує Акт про штучний інтелект, 2024 року (Artificial Intelligence Act) [18], який почне повністю застосовуватися в серпні 2026 року, встановлюючи глобальні стандарти регулювання. Він запроваджує ризик-орієнтований підхід до використання ШІ. Це дозволяє поєднати інноваційний розвиток із захистом фундаментальних прав, включаючи право на недискримінацію та прозорість алгоритмічних рішень. Акт використовує класифікацію систем ШІ за рівнем ризику, що дозволяє

диференційовано підходити до їх регулювання. Наприклад, системи, що використовуються у виборчих процесах або для впливу на громадську думку, підпадають під категорію високого ризику і повинні відповідати суворим вимогам прозорості. Водночас надмірне регулювання може стримувати інновації, що є предметом критики з боку бізнесу. ЄС намагається врівноважити ці аспекти через гнучкі механізми впровадження та пілотні проєкти.

У контексті політичного процесу алгоритми дедалі більше впливають на формування громадської думки та доступ до інформації. Проте, як зазначено у «White Paper on AI», необхідно забезпечити прозорість алгоритмів і підзвітність їх використання, щоб уникнути дискримінації та зловживань [22].

Дослідження Об'єднаного дослідницького центру Європейської комісії (Joint Research Centre, JRC) також підкреслюють важливість довіри як ключового елементу цифрової демократії: без належного рівня захисту даних громадяни не готові активно використовувати цифрові інструменти участі [21]. У цьому контексті виникає парадокс: підвищення рівня безпеки часто супроводжується обмеженням відкритості, і навпаки.

Разом із тим досвід ЄС виявляє і низку суперечностей. Посилення регулювання та контролю за цифровими платформами може створювати ризики надмірного втручання держави у сферу свободи слова. Крім того, прагнення до цифрового суверенітету іноді вступає в конфлікт із принципами відкритого інтернету та глобальної взаємодії. Це підкреслює складність досягнення балансу між безпекою та прозорістю.

Для України, яка активно розвиває цифрове врядування та впроваджує електронні сервіси, питання балансу між безпекою даних і прозорістю політичного процесу є особливо актуальним. В умовах війни цифровізація одночасно створює нові можливості для ефективного управління та посилює ризики кіберзагроз і інформаційних атак. Це зумовлює необхідність комплексного підходу, що поєднує розвиток кібербезпеки, гармонізацію законодавства з європейськими стандартами, зміцнення цифрової довіри та міжнародну співпрацю. Досвід ЄС демонструє ефективність людиноцентричної моделі цифрового врядування, однак підтверджує, що баланс між захистом даних і відкритістю політичного процесу потребує постійного вдосконалення механізмів регулювання.

Висновки і перспективи подальших досліджень. Цифрова суверенність та е-демократія постають як фундаментальні, взаємозалежні вектори сучасної політичної трансформації, чия ефективна синергія можлива лише за умови досягнення динамічного балансу між захистом персональних даних, гарантуванням кібербезпеки та забезпеченням прозорості політичного процесу. Досвід Європейського Союзу слугує ключовим орієнтиром у цьому напрямі, демонструючи життєздатність моделі «людиноцентричної цифровізації», де поєднання нормативної сили (зокрема General Data Protection Regulation, Digital Services Act та Artificial Intelligence Act Act) із прагненням до технологічної автономії дозволяє створити середовище, у якому захист прав людини стає базовою передумовою демократичного розвитку, а не перешкодою для нього.

Ризики цифрової суверенності та е-демократії пов’язані з кіберзагрозами, дезінформацією, порушенням балансу між приватністю та прозорістю, алгоритмічною непрозорістю ШІ, технологічною залежністю та низьким рівнем цифрової довіри громадян. Для ЄС основним викликом є збереження балансу між регулюванням та інноваціями, тоді як для України – із забезпечення цифрової безпеки в умовах війни та протидія гібридним загрозам. Подолання цих ризиків та забезпечення цифрової суверенності потребує інтегрованого підходу, який охоплює правові, технологічні та інституційні механізми, дозволяючи державі переходити від пасивного технічного захисту до стратегічної цифрової стійкості перед обличчям таких загрози, як дезінформаційні операції, алгоритмічна непрозорість штучного інтелекту та домінування глобальних платформ-монополістів.

В умовах гібридних загроз для України стратегічним завданням є зміцнення цифрової інфраструктури та гармонізація законодавства з європейськими стандартами з урахуванням потреб воєнного стану. Пріоритетами є посилення кіберзахисту державних реєстрів, розвиток національної хмарної та ІТ-інфраструктури, забезпечення прозорості алгоритмів цифрових сервісів і незалежний аудит систем штучного інтелекту. Водночас необхідно розширювати медіаграмотність для протидії діпфейкам і дезінформації, підтримувати інструменти електронної демократії з надійною eID-ідентифікацією та поглиблювати партнерство з ЄС у сфері цифрової стійкості. Така адаптація європейських практик дозволить сформувати стійку цифрову екосистему, здатну протидіяти маніпулятивним технологіям і розширювати простір демократичного врядування. Подальші наукові розвідки у цій сфері мають бути зосереджені на аналізі трансформаційного впливу штучного

інтелекту на виборчі процеси, розробці моделей цифрової резистентності суспільства, вивченні блокчейн-технологій як інструментів зміцнення довіри до демократичних інститутів, а також на еволюції поняття цифрового суверенітету в умовах глобальної боротьби за технологічне лідерство.

Бібліографічний список:

1. Антонова О.В., Шаталов С.О. (2025). Електронна демократія та цифрова держава як інструменти громадянського суспільства в Україні. *Проблеми сучасних трансформацій. Серія право публічне управління та адміністрування*. № 15. URL: https://doi.org/10.54929/2786-5746-2025-15-02-04
2. Войнова Е.О. (2021). Електронна демократія: трансформація осмислення. *Політичне життя*. № 4. С. 21-29. URL: https://doi.org/10.31558/2519-2949.2020.4.3
3. Кірін Р. С. (2025). Проблеми розвитку права електронної демократії та електронного урядування міст в Україні. Аналітично-порівняльне правознавство. Том 1 № 6. С. 161-176. URL: https://doi.org/10.24144/2788-6018.2025.06.1.24
4. Крилова Ю.І. (2022). Електронна демократія в Україні: теоретичний і практичний аспекти. Інформація і право. № 2(41). С. 70-77. URL: https://doi.org/10.37750/2616-6798.2022.2(41).270366
5. Петров П.Г. (2025). Демократія онлайн: виклики і можливості політичної участі в умовах цифрової держави. *Acta Securitatae Volynienses*. № 5. С. 80-87. URL: https://doi.org/10.32782/2786-9385/2025-5-11
6. Симисенко І. (2025). Політична участь та електронна демократія: виклики в умовах російського вторгнення в Україну. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління.* № 1(77). С. 169-175. URL: https://doi.org/10.32689/2523-4625-2025-1(77)-24
7. Шебанов В. (2025). Концептуалізація поняття «цифрова демократія» у сучасному науковому дискурсі. *Аспекти публічного управління*. № 13(1). С. 93-105. URL: https://doi.org/10.15421/152511
8. 1st EEAS Report on Foreign Information Manipulation and Interference Threats (2023). *EEAS*. URL: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
9. Czerniawski M. (2025). EU's Digital Sovereignty and the Rights-Based Imperative: Linking Enforcement, Competences and Fundamental Rights. VerfBlog. 2025/12/03. URL: https://dx.doi.org/10.59704/221c82ced6d670b6
10. EDPS Opinions on the Digital Services Act and the Digital Markets Act (2021). *European Data Protection Supervisor*. URL: https://www.edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opinions-digital-services-act-and-digital_en].
11. ENISA Threat Landscape 2024. *ENISA*. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
12. Europe's Digital Decade: Digital Targets for 2030 (2021). *European Commission.* URL: www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/europes-digital-decade-2030-digital-targets
13. European Commission. State of the Digital Decade 2024 Report. Brussels, 2024. URL: https://digital-strategy.ec.europa.eu/en/library/report-state-digital-decade-2024
14. Floridi L., Cath C., Taddeo M. (2018). Digital Ethics: Its Nature and Scope. *The 2018 Yearbook of the Digital Ethics Lab*. P. 9-17. https://doi.org/10.1007/978-3-030-17152-0_2
15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *EUR-Lex*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
16. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925
17. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). *EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
18. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). *EUR-Lex* https://eur-lex.europa.eu/eli/reg/2024/1689/oj
19. Sign or start a European citizens' initiative. *European Citizens' Initiative*. https://citizens-initiative.europa.eu/index_en
20. Ten issues to watch in 2026 : in-depth analysis / S. Sheil et al.; ed. by I. Gaudeul-Ehrhart; European Parliamentary Research Service. Belgium: European Union, 2026. 25 p. URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2026/782587/EPRS_IDA(2026)782587_EN.pdf
21. The Future of Government 2030+. A Citizen Centric Perspective on New Government Models. Luxembourg, 2019. 102 p. *Joint Research Centre (JRC).* URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC115008
22. White Paper on Artificial Intelligence: a European approach to excellence and trust (2020). *European Commission*. URL: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

References:

1. Antonova O.V., Shatalov S.O. (2025). Elektronna demokratiia ta tsyfrova derzhava yak instrumenty hromadianskoho suspilstva v Ukraini. *Problemy suchasnykh transformatsii. Seriia pravo publichne upravlinnia ta administruvannia*. № 15. URL: https://doi.org/10.54929/2786-5746-2025-15-02-04 [in Ukrainian].

2. Voinova E.O. (2021). Elektronna demokratiia: transformatsiia osmyslennia. *Politychne zhyttia*. № 4. S. 21-29. URL: https://doi.org/10.31558/2519-2949.2020.4.3 [in Ukrainian].

3. Kirin R. S. (2025). Problemy rozvytku prava elektronnoi demokratii ta elektronnoho uriaduvannia mist v Ukraini. *Analitychno-porivnialne pravoznavstvo*. Tom 1 № 6. S. 161-176. URL: https://doi.org/10.24144/2788-6018.2025.06.1.24 [in Ukrainian].

4. Krylova Yu.I. (2022). Elektronna demokratiia v Ukraini: teoretychnyi i praktychnyi aspekty. *Informatsiia i pravo*. № 2(41). S. 70-77. URL: https://doi.org/10.37750/2616-6798.2022.2(41).270366 [in Ukrainian].

5. Petrov P.H. (2025). Demokratiia onlain: vyklyky i mozhlyvosti politychnoi uchasti v umovakh tsyfrovoi derzhavy. *Acta Securitatae Volynienses*. № 5. C. 80-87. URL: https://doi.org/10.32782/2786-9385/2025-5-11 [in Ukrainian].

6. Symysenko I. (2025). Politychna uchast ta elektronna demokratiia: vyklyky v umovakh rosiiskoho vtorhnennia v Ukrainu. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia*. № 1(77). S. 169-175. URL: https://doi.org/10.32689/2523-4625-2025-1(77)-24 [in Ukrainian].

7. Shebanov V. (2025). Kontseptualizatsiia poniattia «tsyfrova demokratiia» u suchasnomu naukovomu dyskursi. *Aspekty publichnoho upravlinnia*. № 13(1). S. 93-105. URL: https://doi.org/10.15421/152511 [in Ukrainian].

8. 1st EEAS Report on Foreign Information Manipulation and Interference Threats (2023). EEAS. URL: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

9. Czerniawski M. (2025). EU's Digital Sovereignty and the Rights-Based Imperative: Linking Enforcement, Competences and Fundamental Rights. VerfBlog. 2025/12/03. URL: https://dx.doi.org/10.59704/221c82ced6d670b6

10. EDPS Opinions on the Digital Services Act and the Digital Markets Act (2021). European Data Protection Supervisor. URL: https://www.edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opinions-digital-services-act-and-digital_en

11. ENISA Threat Landscape 2024. ENISA. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

12. Europe's Digital Decade: Digital Targets for 2030 (2021). European Commission. URL: www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/europes-digital-decade-2030-digital-targets

13. European Commission. State of the Digital Decade 2024 Report. Brussels, 2024. URL: https://digital-strategy.ec.europa.eu/en/library/report-state-digital-decade-2024

14. Floridi L., Cath C., Taddeo M. (2018). Digital Ethics: Its Nature and Scope. The 2018 Yearbook of the Digital Ethics Lab. P. 9-17. https://doi.org/10.1007/978-3-030-17152-0_2

15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

16. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925

17. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). EUR-Lex. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

18. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). EUR-Lex https://eur-lex.europa.eu/eli/reg/2024/1689/oj

19. Sign or start a European citizens' initiative. European Citizens' Initiative. https://citizens-initiative.europa.eu/index_en

20. Ten issues to watch in 2026 : in-depth analysis / S. Sheil et al.; ed. by I. Gaudeul-Ehrhart; European Parliamentary Research Service. Belgium: European Union, 2026. 25 p. URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2026/782587/EPRS_IDA(2026)782587_EN.pdf

21. The Future of Government 2030+. A Citizen Centric Perspective on New Government Models. Luxembourg, 2019. 102 p. Joint Research Centre (JRC). URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC115008

22. White Paper on Artificial Intelligence: a European approach to excellence and trust (2020). European Commission. URL: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

Kosenko M. Digital sovereignty and e-democracy: the balance between data security and transparency of the political process

The article provides a comprehensive analysis of the interrelationship between digital sovereignty and e-democracy in the context of the rapid digitalisation of political processes. The study focuses on identifying a critical balance between the need to ensure cybersecurity and the protection of personal and state data, on the one hand, and the preservation of transparency and openness in political processes, on the other. It is substantiated that digital sovereignty is a multidimensional concept encompassing technological control over infrastructure, regulatory governance of the digital space, and the political autonomy of states within the global digital environment. E-democracy is conceptualised as an instrument for enhancing citizens' political participation, strengthening governmental accountability, and reinforcing public trust in governing institutions. The EU experience is analysed as a leading model of "human-centred digitalisation", grounded in the combination of high data protection standards, regulation of digital platforms, and the strategic development of artificial intelligence. It is demonstrated that the EU seeks to simultaneously ensure technological autonomy and safeguard democratic rights; however, it faces challenges related to algorithmic opacity, disinformation, and dependence on global technology corporations. Particular attention is devoted to mechanisms for countering information threats and to the development of digital participation tools, including e-voting, petitions, and open data platforms. It is determined that for Ukraine, the issue of balancing security and transparency is of particular relevance in the context of war and hybrid threats. The necessity of harmonising national legislation with European standards, strengthening cybersecurity, developing digital infrastructure, and enhancing citizens' digital trust is emphasised. It is concluded that an effective model of digital sovereignty and e-democracy is only possible through an integrated approach combining legal, technological, and institutional mechanisms.

Keywords: *digital sovereignty, e-democracy, cybersecurity, data protection, disinformation, digital platforms, artificial intelligence, transparency, digital resilience, EU.*