Двойленко Іван Володимирович

Цифрова держава у системі національної безпеки: політичні механізми та інструменти реалізації

УДК 321.01:004.9:35.078.3:351.86
DOI https://doi.org/10.24195/2414-9616.2026-2.3

Двойленко Іван Володимирович
аспірант
Українського державного університету імені Михайла Драгоманова
вул. Пирогова, 9, Київ, Україна
ORCID: 0009-0007-9285-5186

У статті здійснено політологічний аналіз цифрової держави як складника системи національної безпеки та визначено її місце в сучасних трансформаційних процесах публічного управління. Метою дослідження є з'ясування політичних механізмів і практичних інструментів реалізації цифрової держави в умовах зростання ролі інформаційних і кібернетичних загроз, а також обґрунтування її значення як чинника стійкості, керованості та безпеки держави.

У результаті дослідження встановлено, що цифрова держава є не лише інструментом технічної модернізації адміністративних процедур, а й чинником глибокої трансформації самої логіки політичного управління. У статті показано еволюцію від електронного урядування, орієнтованого переважно на автоматизацію послуг, до цифрового врядування, яке передбачає інтеграцію інформаційних систем, зміну управлінських практик і розширення участі громадян у політичних процесах.

Обґрунтовано, що в системі національної безпеки цифрова держава має подвійний статус: з одного боку, вона сама є об'єктом захисту, а з іншого – інструментом забезпечення безпеки. Її значення виявляється у здатності забезпечувати безперервність управління в кризових умовах, координацію між органами влади, оперативне реагування на загрози, контроль за інформаційними потоками та захист критичної інфраструктури. Окрему увагу приділено цифровому суверенітету як передумові політичної незалежності держави, а також нормативно-правовим, інституційним і демократичним механізмам реалізації цифрової політики.

Водночас у статті визначено ключові інструменти функціонування цифрової держави, серед яких електронні сервіси, державні електронні реєстри, цифрові системи ідентифікації, платформи електронної демократії, засоби кіберзахисту та аналітичні системи на основі великих даних. Доведено, що їх використання сприяє підвищенню прозорості, зниженню бюрократичного навантаження, мінімізації корупційних ризиків та більшій обґрунтованості управлінських рішень.

У висновку встановлено, що цифрова держава в сучасних умовах є не допоміжним, а стратегічним елементом системи національної безпеки. Її ефективний розвиток можливий лише за умови збалансованого поєднання технологічної модернізації, належного правового регулювання, інституційної спроможності, кіберстійкості та демократичного контролю.

Ключові слова: *цифрова держава, національна безпека, цифрове врядування, електронне урядування, кібербезпека, інформаційна безпека, цифровий суверенітет, електронна демократія.*

Вступ. Цифровізація сучасного суспільства зумовлює глибокі трансформації у функціонуванні держави, змінюючи підходи до публічного управління, взаємодії влади і громадян та реалізації державної політики. Формування цифрової держави відбувається під впливом розвитку інформаційно-комунікаційних технологій, що сприяє підвищенню ефективності управлінських процесів, прозорості діяльності інституцій та розширенню можливостей громадянської участі. У цьому контексті цифрова трансформація набуває не лише технологічного, а й політичного значення.

Водночас посилення ролі цифрових технологій актуалізує питання національної безпеки, оскільки поряд із новими можливостями виникають і нові загрози, пов'язані з кіберзлочинністю, дезінформацією та вразливістю цифрової інфраструктури. Це обумовлює необхідність комплексного осмислення цифрової держави як елемента безпекової системи, здатного забезпечувати стійкість, керованість і захист національних інтересів у сучасних умовах.

Мета та завдання. Мета статті полягає у визначенні ролі цифрової держави в системі національної безпеки та обґрунтуванні політичних механізмів і інструментів її реалізації. Завданнями є аналіз сутності цифрової держави, дослідження її інституційних і безпекових характеристик, а також виявлення ключових викликів і перспектив розвитку.

Методи дослідження. Методологічно дослідження цифрової держави доцільно здійснювати з використанням системного підходу, який дозволяє розглядати її як сукупність взаємопов'язаних елементів, що функціонують у межах єдиної політичної системи. Інституційний підхід дає можливість проаналізувати структуру та функції державних органів, відповідальних за реалізацію цифрової політики, а також їхню взаємодію з іншими суб'єктами. Водночас безпековий підхід дозволяє оцінити цифрову державу крізь призму її здатності забезпечувати захист національних інтересів у нових умовах, де інформаційні та кібернетичні загрози відіграють визначальну роль. Поєднання цих підходів формує комплексну теоретико-методологічну основу дослі-

дження, що враховує як інституційні, так і функціональні характеристики цифрової держави.

Результати. Цифрова держава – явище, що формується на перетині розвитку інформаційних технологій та трансформації публічної політики. Цифрова держава виступає не лише інструментом оптимізації адміністративних процесів, але й фактором зміни логіки політичного управління, що набуває більш відкритого, інтерактивного та орієнтованого на дані характеру.

Аналіз концепцій електронного урядування та цифрового врядування дозволяє простежити еволюцію підходів до цифровізації держави. Якщо електронне урядування зосереджується на автоматизації окремих адміністративних процедур та наданні послуг у цифровій формі, то цифрове врядування передбачає глибшу трансформацію управлінських процесів, включаючи інтеграцію інформаційних систем, зміну управлінських практик та підвищення рівня участі громадян [8].

У структурі національної безпеки цифрова держава посідає особливе місце, оскільки виступає одночасно і об'єктом захисту, і інструментом забезпечення безпеки. З одного боку, цифрова інфраструктура потребує надійного захисту від кіберзагроз та інформаційних атак, з іншого боку вона забезпечує ефективність управління кризовими ситуаціями, підвищує рівень координації між органами влади та сприяє оперативному прийняттю рішень.

Цифрова держава як елемент системи національної безпеки набуває дедалі більшого значення в умовах зростання ролі інформаційного простору у сучасних політичних процесах. Традиційні підходи до національної безпеки, які зосереджувалися переважно на військових та економічних аспектах, поступово доповнюються новими вимірами, пов'язаними з інформаційною та кібернетичною безпекою. У цьому контексті цифрова держава виступає як ключовий інструмент забезпечення контролю над інформаційними потоками, захисту критичної інфраструктури та протидії дезінформації [6].

Важливою характеристикою цифрової держави є її здатність забезпечувати безперервність управління в умовах кризових ситуацій. Використання цифрових інструментів дозволяє зберігати ефективність управління навіть за умов обмеження фізичної присутності або руйнування традиційної інфраструктури.

Суттєвим аспектом є взаємозв'язок між рівнем розвитку цифрової інфраструктури та здатністю держави протидіяти сучасним загрозам. Розвинені інформаційні системи дозволяють здійснювати моніторинг ситуації в реальному часі, оперативно реагувати на загрози та координувати дії різних органів влади. Водночас залежність від цифрових технологій створює нові ризики, пов'язані з можливістю кібератак, витоків даних та втручання у функціонування державних систем.

У цьому контексті важливого значення набуває поняття цифрового суверенітету, яке передбачає здатність держави самостійно контролювати свої інформаційні ресурси, інфраструктуру та цифрові платформи. Забезпечення цифрового суверенітету є необхідною умовою збереження політичної незалежності та захисту національних інтересів у глобалізованому світі [4].

Цифровізація суттєво трансформує класичні уявлення про національну безпеку, зміщуючи акценти з переважно військових і територіальних аспектів у бік інформаційних, кібернетичних та комунікаційних вимірів. У сучасних умовах саме контроль над інформаційними потоками, захист цифрової інфраструктури та здатність до швидкої комунікації стають визначальними факторами безпеки держави.

Цифрова держава у цьому контексті виступає як інтеграційна платформа, що поєднує різні компоненти безпекової політики та забезпечує їхню узгоджену реалізацію. Вона створює нові можливості для моніторингу загроз, аналізу ризиків і прийняття управлінських рішень на основі актуальних даних.

Водночас цифровізація створює нові виклики, пов'язані з підвищенням вразливості держави до кіберзагроз та інформаційних атак. У цьому контексті ключового значення набуває кібербезпека як здатність держави захищати свої інформаційні системи від несанкціонованого доступу, втручання або руйнування. Паралельно формується концепція інформаційної безпеки, що охоплює захист інформаційного простору від маніпуляцій, дезінформації та пропагандистського впливу [2].

Окрему роль відіграє поняття цифрового суверенітету, яке передбачає здатність держави контролювати власну цифрову інфраструктуру, дані та технологічні ресурси. Забезпечення такого суверенітету є необхідною умовою збереження політичної незалежності, особливо в умовах глобалізації та залежності від транснаціональних технологічних компаній. Таким чином, цифрова держава виступає не лише як інструмент модернізації управління, але і як ключовий компонент системи національної безпеки, що визначає здатність держави ефективно реагувати на сучасні виклики.

Формування безпечної цифрової держави передбачає реалізацію комплексу політичних механізмів, спрямованих на забезпечення її ефективного функціонування та захисту від загроз. Одним із ключових механізмів є нормативно-правове регулювання, яке визначає правила функціонування цифрового середовища, встановлює стандарти безпеки та регламентує використання інформаційних технологій у публічному управлінні [13].

Важливу роль відіграє стратегічне планування, що передбачає визначення довгострокових пріо-

ритетів цифрової трансформації та узгодження їх із цілями національної безпеки. Ефективність цих документів значною мірою залежить від рівня їхньої реалізації та координації між різними органами державної влади. У цьому контексті особливого значення набуває інституційна взаємодія, яка забезпечує узгодженість дій різних суб'єктів та запобігає дублюванню функцій.

Не менш важливим є механізм інституційного забезпечення, який передбачає створення та розвиток спеціалізованих органів, відповідальних за цифрову трансформацію та кібербезпеку. Їхня діяльність має бути спрямована не лише на впровадження технологічних рішень, але й на формування політики, координацію дій та забезпечення контролю за дотриманням встановлених стандартів. Водночас важливо забезпечити належний рівень підзвітності та прозорості їхньої діяльності, що сприяє підвищенню довіри з боку суспільства.

Окрему роль відіграють механізми демократичного контролю та участі громадян, які забезпечують легітимність цифрової політики та сприяють врахуванню суспільних інтересів. Використання цифрових інструментів участі дозволяє залучати громадян до процесу прийняття рішень, підвищувати рівень прозорості та зміцнювати взаємодію між державою і суспільством [12].

Реалізація цифрової держави у безпековому вимірі забезпечується через систему практичних інструментів, які інтегрують технологічні рішення у процеси публічного управління та створюють умови для підвищення ефективності функціонування державних інституцій. Одним із базових елементів виступають електронні сервіси, що забезпечують доступ громадян до адміністративних послуг у цифровому форматі.

Їхнє впровадження сприяє спрощенню процедур, зменшенню бюрократичного навантаження та мінімізації безпосереднього контакту між громадянином і представником влади, що у свою чергу знижує ризики корупційних практик. Електронні сервіси також підвищують прозорість діяльності органів державної влади, оскільки дозволяють відстежувати процес надання послуг і контролювати строки їх виконання.

Важливим інструментом є державні електронні реєстри, які акумулюють та систематизують інформацію про різні сфери суспільного життя. Їх інтеграція забезпечує єдність інформаційного простору держави, сприяє обміну даними між органами влади та підвищує оперативність прийняття рішень. У безпековому контексті такі реєстри відіграють ключову роль у забезпеченні контролю за ресурсами, виявленні загроз та запобіганні правопорушенням [14].

Цифрові ідентифікаційні системи є ще одним важливим компонентом цифрової держави, оскільки забезпечують надійну верифікацію особи у цифровому середовищі. Вони створюють передумови для безпечного доступу до державних сервісів, здійснення електронних транзакцій та реалізації інструментів електронної демократії.

Платформи електронної демократії, своєю чергою, розширюють можливості участі громадян у політичних процесах, сприяють підвищенню рівня прозорості та підзвітності влади. Використання таких платформ дозволяє залучати громадян до обговорення та ухвалення рішень, що зміцнює легітимність політичної системи [1].

Особливого значення набувають інструменти кіберзахисту, які забезпечують стійкість цифрової інфраструктури до зовнішніх і внутрішніх загроз. До них належать системи виявлення та запобігання кібератакам, засоби шифрування даних, а також механізми резервного зберігання інформації. Важливим елементом є створення систем моніторингу та реагування на інциденти, що дозволяє оперативно виявляти загрози та мінімізувати їхні наслідки.

Сучасні тенденції розвитку цифрової держави пов'язані з активним використанням великих даних та аналітичних систем. Застосування цих технологій дозволяє здійснювати глибокий аналіз соціально економічних процесів, прогнозувати розвиток ситуацій та підвищувати обґрунтованість управлінських рішень. Використання аналітичних інструментів сприяє підвищенню ефективності державної політики, оскільки дозволяє враховувати значні обсяги інформації та виявляти приховані закономірності [3].

Разом з тим, розвиток цифрової держави у контексті національної безпеки супроводжується низкою викликів і ризиків, які мають комплексний характер і охоплюють як технологічні, так і політичні аспекти. Однією з ключових загроз є зростання кіберзлочинності та активізація кібератак, спрямованих на критичну інфраструктуру, державні інформаційні системи та бази даних.

Вразливість цифрових систем створює ризики порушення функціонування державного управління, що особливо небезпечно в умовах кризових ситуацій. Поряд із цим значною проблемою залишаються витоки даних, які можуть призводити до компрометації персональної інформації громадян і підриву довіри до державних інституцій.

Суттєвим викликом є залежність від технологічних платформ та іноземних цифрових рішень, що обмежує можливості держави щодо контролю над власною інформаційною інфраструктурою. Така залежність може створювати додаткові ризики у сфері національної безпеки, оскільки критично важливі сервіси можуть опинитися під впливом зовнішніх суб'єктів [5].

Не менш важливим є питання цифрової нерівності, яка проявляється у нерівному доступі різних соціальних груп до цифрових технологій та послуг. Це призводить до соціальної диференціації та обмеження участі окремих категорій громадян у політичному та суспільному житті.

Окрему групу становлять політичні ризики, пов'язані з використанням цифрових технологій для маніпуляції інформацією та впливу на громадську думку. Поширення дезінформації, використання алгоритмічних механізмів для таргетування аудиторій та втручання у виборчі процеси створюють загрозу для демократичних інститутів. У цьому контексті особливого значення набуває забезпечення інформаційної безпеки та розвиток механізмів протидії маніпулятивному впливу [11].

Важливою проблемою є також забезпечення захисту персональних даних та дотримання прав громадян у цифровому середовищі. Зростання обсягів обробки даних потребує встановлення чітких правових норм і ефективних механізмів контролю за їх дотриманням. Недостатній рівень захисту призводить до зловживань та порушення права на приватність, що негативно впливає на рівень довіри до цифрових інструментів держави.

Попри наявні ризики, розвиток цифрової держави відкриває значні перспективи для зміцнення національної безпеки. Одним із ключових напрямів є інтеграція у європейський цифровий простір, що передбачає гармонізацію стандартів, обмін досвідом та участь у спільних безпекових ініціативах. Важливим є також посилення кіберстійкості через розвиток національних систем захисту, підготовку фахівців та впровадження сучасних технологій. Таким чином, за умови належного врахування ризиків і формування збалансованої політики цифрова держава може стати важливим чинником забезпечення стійкості та безпеки сучасної держави.

Висновки. У результаті дослідження встановлено, що цифрова держава трансформується у ключовий елемент системи національної безпеки, поєднуючи функції інструмента управління та об'єкта захисту. Її розвиток змінює традиційні підходи до публічної політики, зумовлюючи перехід до відкритих, інтегрованих і даноорієнтованих моделей управління.

Визначено, що ефективність цифрової держави залежить від узгодженості нормативно-правового регулювання, інституційної спроможності органів влади, рівня розвитку цифрової інфраструктури та здатності забезпечувати кібер- й інформаційну безпеку. Особливого значення набуває цифровий суверенітет як умова збереження політичної незалежності та контролю над національними інформаційними ресурсами.

Доведено, що впровадження цифрових інструментів сприяє підвищенню прозорості, ефективності управління та залученню громадян до політичних процесів. Водночас встановлено наявність комплексних ризиків, пов'язаних із кібератаками, витоками даних, технологічною залежністю та маніпуляціями інформацією. Це обумовлює необхідність формування збалансованої державної політики, що поєднує інноваційний розвиток із забезпеченням безпеки, захистом персональних даних і дотриманням прав громадян у цифровому середовищі.

Перспективи подальших досліджень доцільно пов'язати з поглибленим аналізом механізмів забезпечення цифрового суверенітету в умовах глобальної технологічної залежності, оцінкою ефективності державних політик у сфері кібербезпеки, а також вивченням впливу цифрових платформ на демократичні процеси та політичну стабільність.

ЛІТЕРАТУРА:

1. Антонова О. В., Шаталов С. О. Електронна демократія та цифрова держава як інструменти громадянського суспільства в Україні. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2025. № 15. URL: https://doi.org/10.54929/2786-5746-2025-15-02-04.

2. Братах Л. Інформаційна безпека України в умовах дезінформаційного впливу: загрози, виклики, механізми реагування. *Вісник прикарпатського університету. серія: політологія*. 2025. № 21. С. 50–59. URL: https://doi.org/10.32782/2312-1815/2025-21-6.

3. Була Р. Роль відкритих даних у розвитку цифрової держави. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2025. № 1(77). С. 31–37. URL: https://doi.org/10.32689/2523-4625-2025-1(77)-5.

4. Горлинський В., Горлинський Б. Кібервійна як системний виклик кібербезпеці України. *Information technology and security*. 2025. № 13. С. 118–133. URL: https://ela.kpi.ua/server/api/core/bitstreams/104512e0-daf1-4a10-9c49-5d635cd2b318/content.

5. Милосердна І. Цифровий суверенітет держави: наукова риторика та реальні зміни. *Науковий журнал «Політикус»*. 2024. № 6. С. 154–160. URL: https://politicus.od.ua/6_2024/25.pdf.

6. Новікова Н. Л., Бойко Л. В. Цифровізація та національна безпека: тенденції та виклики. *National security law and economics*. 2024. № 1. С. 71–76. URL: https://doi.org/10.51369/3083-5917-2024-1-8.

7. Олексюк Р.В. Цифрова трансформація та цифрова економіка – шлях розвитку економіки в умовах глобалізації. *Економічні науки. Серія «Регіональна економіка»*. 2025. Т. 1, № 21(83). С. 223–229. URL: https://doi.org/10.36910/2707-6296-2024-21(83)-24.

8. Решетова Г. Електронне урядування як складова інформаційно- комунікаційної системи забезпечення сталого розвитку. *Public administration and regional development*. 2022. № 18. С. 1141–1162. URL: https://doi.org/10.34132/pard2022.18.08.

9. Талдикін О. Інформаційний суверенітет та його зміст. *Naukovyy visnyk dnipropetrovskogo derzhavnogo universytety vnutrishnikh sprav*. 2024. № 2. С. 132–138. URL: https://doi.org/10.31733/2078-3566-2023-2-132-138.

10. Khudoliy A. Cybersecurity: modern challenges of Ukraine. *Acta de historia & politica: saeculum XXI*. 2020. № 01. С. 138–146. URL: https://doi.org/10.26693/ahpsxxi2019.01.138.

11. Kushnir I. P., Adamchuk S. V. Countering disinformation: organizational and legal aspect. *Analytical and comparative jurisprudence*. 2025. № 1. С. 470–475. URL: https://doi.org/10.24144/2788-6018.2025.01.78.

12. Orlovska Y., Larionova K. The concept of the formation the electronic democracy as a tool of regional public administration. *Economic scope*. 2024. № 192. С. 102–108. URL: https://doi.org/10.30838/ep.192.102-108.

13. Slyvka M. M., Lukianova H. Y. Legal provision of information security: the experience of the countries of the European Union. *Juridical scientific and electronic journal*. 2021. № 11. С. 514–516. URL: https://doi.org/10.32782/2524-0374/2021-11/132.

14. Systematic analysis of the security of state electronic registers and personal databases / O. Zadereyko та ін. *Cybersecurity education science technique*. 2025. С. 57. URL: https://doi.org/10.28925/2663-4023.2025.28.735.

REFERENCES:

1. Antonova, O. V., Shatalov, S. O. (2025). Elektronna demokratiia ta tsyfrova derzhava yak instrumenty hromadianskoho suspilstva v Ukraini [Electronic democracy and digital state as tools of civil society in Ukraine]. Problemy suchasnykh transformatsii. Seriia: pravo, publichne upravlinnia ta administruvannia, 15. https://doi.org/10.54929/2786-5746-2025-15-02-04 [in Ukrainian].

2. Bratakh, L. (2025). Informatsiina bezpeka Ukrainy v umovakh dezinformatsiinoho vplyvu: zahrozy, vyklyky, mekhanizmy reahuvannia [Information security of Ukraine under disinformation influence: threats, challenges, response mechanisms]. Visnyk Prykarpatskoho universytetu. Seriia: politolohiia, 21, 50–59. https://doi.org/10.32782/2312-1815/2025-21-6 [in Ukrainian].

3. Bula, R. (2025). Rol vidkrytykh danykh u rozvytku tsyfrovoi derzhavy [The role of open data in the development of the digital state]. Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia, 1(77), 31–37. https://doi.org/10.32689/2523-4625-2025-1(77)-5 [in Ukrainian].

4. Horlynskyi, V., Horlynskyi, B. (2025). Kiberiina yak systemnyi vyklyk kiberbezpetsi Ukrainy [Cyberwar as a systemic challenge to Ukraine's cybersecurity]. Information technology and security, 13, 118–133. https://ela.kpi.ua/server/api/core/bitstreams/104512e0-daf1-4a10-9c49-5d635cd2b318/content [in Ukrainian].

5. Myloserda, I. (2024). Tsyfrovyi suverenitet derzhavy: naukova rytoryka ta realni zminy [Digital sovereignty of the state: scientific rhetoric and real changes]. Naukovyi zhurnal «Politykus», 6, 154–160. https://politicus.od.ua/6_2024/25.pdf [in Ukrainian].

6. Novikova, N. L., Boiko, L. V. (2024). Tsyfrovizatsiia ta natsionalna bezpeka: tendentsii ta vyklyky [Digitalization and national security: trends and challenges]. National security law and economics, 1, 71–76. https://doi.org/10.51369/3083-5917-2024-1-8 [in Ukrainian].

7. Oleksiuk, R. V. (2025). Tsyfrova transformatsiia ta tsyfrova ekonomika – shliakh rozvytku ekonomiky v umovakh hlobalizatsii [Digital transformation and digital economy as a path of economic development under globalization]. Ekonomichni nauky. Seriia "Rehionalna ekonomika", 1, 21(83), 223–229. https://doi.org/10.36910/2707-6296-2024-21(83)-24 [in Ukrainian].

8. Reshetova, H. (2022). Elektronne uriaduvannia yak skladova informatsiino-komunikatsiinoi systemy zabezpechennia staloho rozvytku [E-government as a component of the information and communication system for sustainable development]. Public administration and regional development, 18, 1141–1162. https://doi.org/10.34132/pard2022.18.08 [in Ukrainian].

9. Taldykin, O. (2024). Informatsiinyi suverenitet ta yoho zmist [Information sovereignty and its content]. Naukovyy visnyk Dnipropetrovskoho derzhavnoho universytetu vnutrishnikh sprav, 2, 132–138. https://doi.org/10.31733/2078-3566-2023-2-132-138 [in Ukrainian].

10. Khudoliy, A. (2020). Cybersecurity: modern challenges of Ukraine. Acta de historia & politica: saeculum XXI, 01, 138–146. https://doi.org/10.26693/ahpsxxi2019.01.138.

11. Kushnir, I. P., Adamchuk, S. V. (2025). Countering disinformation: organizational and legal aspect. Analytical and comparative jurisprudence, 1, 470–475. https://doi.org/10.24144/2788-6018.2025.01.78.

12. Orlovska, Y., Larionova, K. (2024). The concept of the formation of electronic democracy as a tool of regional public administration. Economic scope, 192, 102–108. https://doi.org/10.30838/ep.192.102-108.

13. Slyvka, M. M., Lukianova, H. Y. (2021). Legal provision of information security: the experience of the countries of the European Union. Juridical scientific and electronic journal, 11, 514–516. https://doi.org/10.32782/2524-0374/2021-11/132.

14. Zadereyko, O., et al. (2025). Systematic analysis of the security of state electronic registers and personal databases. Cybersecurity education science technique, 28, 57. https://doi.org/10.28925/2663-4023.2025.28.735.

Digital state in the system of national security: political mechanisms and instruments of implementation

Dvoylenko Ivan Volodymyrovych

Postgraduate Student
Mykhailo Drahomanov Ukrainian State University
Pirogov str., 9, Kyiv, Ukraine
ORCID: 0009-0007-9285-5186

The article provides a political science analysis of the digital state as a component of the national security system and determines its place within contemporary transformations of public governance. The purpose of the study is to identify the political mechanisms and practical instruments for implementing the digital state in the context of the growing role of informational and cyber threats, as well as to substantiate its significance as a factor of state resilience, governability, and security.

The study finds that the digital state is not only a tool for the technical modernization of administrative procedures, but also a driver of a profound transformation in the very logic of political governance. The article demonstrates the evolution from e-government, primarily focused on service automation, to digital governance, which involves the integration of information systems, transformation of management practices, and expansion of citizen participation in political processes.

It is substantiated that within the national security system the digital state has a dual status: on the one hand, it is itself an object of protection, and on the other, it serves as an instrument for ensuring security. Its significance is manifested in its ability to ensure continuity of governance under crisis conditions, coordination among public authorities, rapid response to threats, control over information flows, and protection of critical infrastructure. Particular attention is paid to digital sovereignty as a prerequisite for political independence, as well as to legal, institutional, and democratic mechanisms for implementing digital policy. At the same time, the article identifies key instruments of the digital state's functioning, including electronic services, state electronic registers, digital identification systems, e-democracy platforms, cybersecurity tools, and big data analytics systems. It is proven that their use contributes to increased transparency, reduced bureaucratic burden, minimization of corruption risks, and more evidence-based decision-making.

In conclusion, it is established that in modern conditions the digital state is not an auxiliary but a strategic element of the national security system. Its effective development is possible only under the condition of a balanced combination of technological modernization, proper legal regulation, institutional capacity, cyber resilience, and democratic oversight.

Key words: *digital state, national security, digital governance, e-government, cybersecurity, information security, digital sovereignty, e-democracy.*

Дата першого надходження статті до видання: 10.03.2026
Дата прийняття статті до друку після рецензування: 13.04.2026
Дата публікації (оприлюднення) статті: 21.05.2026