

Конституційне право; муніципальне право

УДК 342.1

DOI <https://doi.org/10.5281/zenodo.15306095>

**Підходи ЄС до формування цифрового суверенітету:
досвід Естонії для України**

Петришина Марина Олександрівна

кандидат юридичних наук, доцент, доцент кафедри державного будівництва

Національний юридичний університет імені Ярослава Мудрого,

61024, вул. Григорія Сковороди, 77, Харків, Україна,

e-mail: m.o.petryshyna@nlu.edu.ua,

ORCID <https://orcid.org/0000-0002-5702-0112>

Балабан Марія Миколаївна

студентка 13 групи, 2 курсу, факультету прокуратури

Національний юридичний університет імені Ярослава Мудрого,

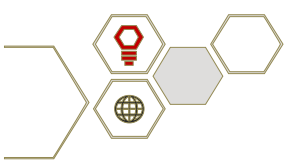
61024, вул. Григорія Сковороди, 77, Харків, Україна,

e-mail: m.m.balaban@nlu.edu.ua,

ORCID <https://orcid.org/0009-0007-8255-4187>

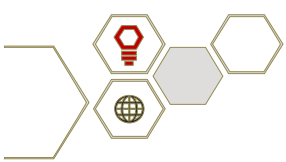
Прийнято: 17.04.2025 | Опубліковано: 29.04.2025

***Анотація.** Мета дослідження полягає у визначенні ролі цифрового суверенітету в умовах сучасних викликів, а також у вивченні європейського досвіду з акцентом на можливості його застосування в Україні під час дії воєнного стану. У роботі розглядається цифровий суверенітет як багатовимірне явище, що охоплює правові, технічні та політичні аспекти. Методологія дослідження ґрунтується на системному аналізі правових актів,*



використанні порівняльно-правового підходу та вивченні підходів держав-членів Європейського Союзу. Аналізу піддаються підходи та нормативно-правові акти, що закладають основи формування моделі цифрового суверенітету Європейського Союзу. Серед них виокремлюються такі, як Закон «Про цифрові послуги», Закон «Про штучний інтелект», DORA та NIS2, Декларація про цифрові права та принципи, а також стратегія «Цифрове десятиліття». Особлива увага приділяється естонському досвіду організації електронного голосування та впровадження програми e-Residency, які демонструють високий рівень інтеграції технологій у публічне управління та бізнес-середовище. У результаті проведеного дослідження встановлюється, що комплексна правова основа, інвестиції в кібербезпеку, а також розвиток цифрової ідентифікації є критично важливими для забезпечення цифрового суверенітету. Досвід ЄС доводить необхідність формування цілісної стратегії цифрового розвитку та адаптації законодавства до нових викликів та загроз. У контексті України наголошується на нагальній потребі вдосконалення чинного законодавства у сфері захисту персональних даних, кібербезпеки, регулювання електронної ідентифікації та підтримки національних технологічних компаній. Висновки дослідження підкреслюють, що цифровий суверенітет є ключовим чинником державної стійкості у воєнний час, а також важливою складовою повоєнного відновлення України. Вказуються потенційні напрямки подальшого удосконалення чинного законодавства України у цій сфері.

Ключові слова: цифровий суверенітет, кібербезпека, електронне голосування, цифрова ідентифікація, правове регулювання, цифрова критична інфраструктура, електронне урядування, захист персональних даних, цифрова трансформація.



The European Union's Approaches to the Formation of Digital Sovereignty: Estonia's Experience for Ukraine

Petryshyna Maryna Oleksandrivna

Ph.D. in Law, Docent, Associate Professor at the Department
of State Building Yaroslav Mudryi National Law University,
61024, vul. Hryhoriia Skovorody, 77, Kharkiv, Ukraine,

e-mail: m.o.petryshyna@nlu.edu.ua,

ORCID <https://orcid.org/0000-0002-5702-0112>

Balaban Mariia Mykolaivna

Student of the 2nd course of the 13th group Faculty of the Prosecutor's Office

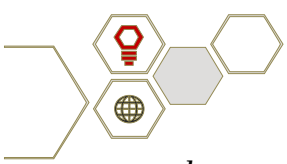
Yaroslav Mudryi National Law University,

61024, vul. Hryhoriia Skovorody, 77, Kharkiv, Ukraine,

e-mail: m.m.balaban@nlu.edu.ua,

ORCID <https://orcid.org/0009-0007-8255-4187>

Abstract. *This study aims to identify the role of digital sovereignty amid contemporary challenges and to analyze the European experience with a focus on its applicability to Ukraine under martial law conditions. Digital sovereignty is examined as a complex phenomenon encompassing legal, technical and political dimensions. The research is based on the systematic analysis of legislative acts, a comparative legal approach, and the study of practices implemented by the European Union Member States. The paper reviews key regulatory frameworks that underpin the EU's model of digital sovereignty, including the Digital Services Act, the Artificial Intelligence Act, DORA, NIS2, the Declaration on Digital Rights and Principles and the Digital Decade strategy. Special emphasis is placed on Estonia's experience in organizing internet voting and implementing the e-Residency program, both demonstrating a high level of technological integration into governance and the business environment. The results of the study reveal that a robust legal framework, sustained investment in*



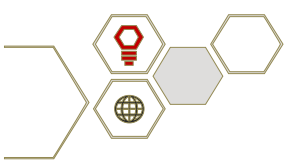
cybersecurity, and the advancement of digital identification systems are essential to safeguarding digital sovereignty. The European experience confirms the need for a comprehensive digital development strategy and the timely adaptation of legislation to new risks and challenges. In the Ukrainian context, the findings stress the urgent need to enhance current legislation regarding personal data protection, cybersecurity, electronic identification, and support for national technology companies. It is concluded that digital sovereignty represents a fundamental component of national resilience during wartime and a critical element for Ukraine's post-war recovery. The study also outlines potential avenues for further improvement of Ukrainian legislation in this domain.

Keywords: *digital sovereignty, cybersecurity, internet voting, digital identification, legal framework, critical digital infrastructure, e-governance, personal data protection, digital transformation.*

Постановка проблеми. У сучасну епоху стрімкого розвитку цифрових технологій інновації з'являються практично щодня, змінюючи різні сфери суспільного життя [1]. Водночас, цифровізація не завжди здійснюється в інтересах суспільства, що обумовлює необхідність відповідного правового регулювання. Право, як універсальний механізм врегулювання суспільних відносин, охоплює й цифрову сферу, забезпечуючи захист прав та інтересів особи в умовах технологічної трансформації.

Особливої актуальності набуває питання цифрового суверенітету – здатності держави забезпечувати контроль над цифровими процесами, захист даних громадян та цифрової інфраструктури [2]. В умовах, коли обробка персональних даних здійснюється на серверах, розташованих за межами національної юрисдикції, а кібератаки перетворюються на інструмент геополітичного впливу, забезпечення цифрового суверенітету стає критично важливим завданням.

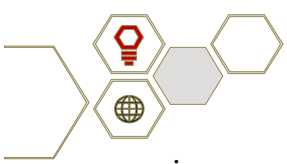
Разом з тим, технологічний розвиток випереджає динаміку правотворчості [3]. Законодавчі системи багатьох держав не встигають оперативно адаптуватися



до нових викликів цифрової доби, що створює ризики правової невизначеності. На цьому тлі особливого значення набувають стратегії та ініціативи, спрямовані на формування сталого та безпечного цифрового середовища. У цьому контексті, досвід ЄС, який активно розробляє політики у сфері цифрового суверенітету, а також Естонії, як однієї з провідних держав у сфері цифровізації, становить значний інтерес для аналізу.

Аналіз останніх досліджень та публікацій свідчить про зростаючий науковий інтерес до проблематики цифрового суверенітету, навіть незважаючи на відносну новизну цієї теми. Власний внесок у її розвиток зробили Юлія Поле та Торстен Тіль, які в своїй колективній праці “Digital Vernetzung und Souveränität” дослідили історичні витоки цифрової взаємодії та нормативні підходи до забезпечення суверенітету в цифровій сфері [4]. На особливу увагу заслуговує нещодавня публікація Люсі Кадлецова «Cyber sovereignty» (липень, 2024), в якій авторка здійснює глибокий аналіз підходів до кіберсуверенітету в різних державах, зокрема, у США, Естонії, Нідерландах та Туреччині [5]. Важливим у розвиток цього напрямку наукового пошуку є внесок авторки Рената Авіло Пінто, яка в роботі “Digital sovereignty or digital colonialism?” порушує питання протистояння цифрового суверенітету та цифрового колоніалізму, розглядаючи загрози стеження та невпинного зростання контролю над суспільством [6]. Цінним є спільне дослідження Стефан Кутюр та Софі Тупін “What does the notion of ‘sovereignty’ mean when referring to the digital?”, в якому автори підкреслюють відсутність уніфікованого визначення поняття цифрового суверенітету та демонструють складність його інтерпретацій у різних правових і політичних контекстах [7].

Окремо слід відзначити дослідження Амстердамського університету “Preserving digital sovereignty of universities and researchers”, в якому наголошується на необхідності забезпечення цифрової автономії не лише держав, а й академічних інституцій. Такий підхід розширює традиційне розуміння цифрового суверенітету, охоплюючи також наукову і освітню сфери [8]. Як бачимо, актуальність проблематики цифрового суверенітету



підтверджується її мультидисциплінарним характером та широкою сферою застосування, що охоплює як публічне управління, так і приватний сектор, освіту та науку.

Виділення невирішених раніше частин загальної проблеми. Варто наголосити на комплексності розвитку законодавства у сфері цифрового суверенітету в Європейському Союзі та успішних практиках, продемонстрованих, зокрема, Естонією. При цьому, й досі залишається низка питань, які не отримали остаточного вирішення. Зокрема, це питання оптимальної адаптації нормативно-правового регулювання до нових викликів, таких, як штучний інтелект, квантові технології, а також посилення кіберзагроз у період воєнних конфліктів. Недостатньо розробленими є й механізми забезпечення цифрової стійкості держави у кризових ситуаціях та гарантування незалежності критичної цифрової інфраструктури. Так, для України, яка сьогодні перебуває у стані війни, ці питання набувають особливої ваги, що обумовлює необхідність розроблення національної моделі цифрового суверенітету, а також удосконалення чинного законодавства з урахуванням досвіду провідних держав та специфіки сучасних викликів.

Сьогодні у глобальній цифровій гонці за контроль над інформацією та технологіями США, Китай та Європейський Союз стали основними гравцями, кожен з яких формує власні стандарти цифрового суверенітету, зокрема, через оновлення правового регулювання в галузі кібербезпеки, даних і цифрових прав. У той час, як авторитарні держави зосереджують зусилля на централізованому контролі та моніторингу інформації, демократичні держави стикаються зі складним завданням – необхідністю пошуку балансу між національною безпекою з одного боку, інноваціями і захистом прав людини з другого.

Підтримуємо ідею щодо використання цифровізації як засобу досягнення більшого добробуту, рівності та здоровішого навколишнього середовища, шляхом розробки цифрової інфраструктури, здатної функціонувати у межах спроможності планети та можливості людей долати перешкоди. Цифровізацію слід використовувати розумно і помірковано, щоб вона сприяла прийняттю



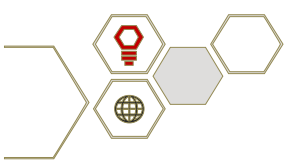
кращих рішень, досягненню кращих результатів та підвищенню спроможності (стійкості) виробництва та споживання [9]. У такому глобальному контексті, що динамічно змінюється і розвивається, досвід таких країн, як Естонія, є надзвичайно цінним. Естонія успішно поєднала інноваційні технології з високими стандартами демократичних прав і свобод, створивши модель цифрового суверенітету, вивчення якої і адаптація до українських реалій може сприяти формуванню власної національної моделі цифрового суверенітету.

Метою цієї статті є вивчення підходів ЄС, а також досвіду Естонії до забезпечення цифрового суверенітету, виявлення основних проблем та тенденцій розвитку відповідного правового регулювання, а також визначення напрямів удосконалення чинного правового регулювання означеної сфери з урахуванням викликів періоду воєнного стану в Україні.

Виклад основного матеріалу. Поняття цифрового суверенітету. Насамперед, слід відзначити, що сьогодні не існує єдиного загальноприйнятого визначення цифрового суверенітету або відповідного комплексного нормативного акту. У зв'язку з означенням, доцільно спиратися на наукові підходи при аналізі досліджуваного явища. Згідно з одним з найпоширеніших визначень під цифровим суверенітетом розуміють здатність держави регулювати технологічну сферу, а також розробляти та впроваджувати інноваційні рішення [10]. За іншого підходу, цифровий суверенітет розглядають як здатність контролювати власну цифрову долю на трьох рівнях: на фізичному (інфраструктура, технології), на рівні коду (стандарти, правила, дизайн), а також на рівні даних (право власності, обробка і використання) [11]. Крім того, цифровий суверенітет можна визначити як контроль за тим, як і де зберігаються дані, що передбачає надання організаціям і особам більшої автономії у сфері управління цифровими активами [12].

Аналізуючи підходи до розуміння та визначення цифрового суверенітету можна дійти висновку, що одним з ключових його аспектів є захист даних.

Цифровий суверенітет Європейського Союзу. Проблематика цифрового суверенітету в Європейському Союзі почала формуватися в середині 1990-х рр.,



зокрема, у вигляді окремих ініціатив у сфері інтернет-політики. Поступовий розвиток цифрових технологій, домінування глобальних сервісів американського походження (таких, як Facebook та Google тощо), став поштовхом для активізації зусиль ЄС щодо посилення захисту прав громадян у цифровому середовищі [13].

Наявні сьогодні кейси свідчать про необхідність розвитку правового регулювання і досліджуваної сфери в цілому. Так, Європейська комісія здійснює розслідування і регулювання діяльності цифрових компаній. Наприклад, на основі Регламенту Р2В, що регулює прозорість у сфері онлайн-посередництва, ЄК здійснила низку заходів, зокрема, у 2019 р. оштрафувала компанію Google за зловживання домінуючим становищем у сфері розміщення онлайн-реклами [14].

У 2024 році було розпочато розслідування проти компанії Тему за можливе порушення Закону «Про цифрові послуги» (DSA) [15], зокрема, це стосується недостатньої боротьби з поширенням незаконного контенту. У цьому контексті, важливо згадати політичні рекомендації президентки Європейської комісії Урсули фон дер Ляєн, яка наголосила на необхідності формування та розвитку цифрових ринків для забезпечення рівних умов конкуренції та захисту прав споживачів. Ця теза є частиною стратегії Європейського Союзу щодо сталого (стійкого), рівного, безпечного та конкурентного ринку у цифровій сфері [16].

Ключові законодавчі ініціативи ЄС у сфері цифрового суверенітету. Європейський Союз розробив комплекс нормативно-правових актів, спрямованих на регулювання цифрової сфери, що охоплює усі ключові сфери суспільного життя. Однією з важливих ініціатив став Закон про цифрову операційну стійкість (DORA), який нещодавно набув чинності. Цим актом встановлюються вимоги до фінансових установ щодо їх стійкості до інформаційно-комунікаційних загроз [17].

Крім того, у сфері штучного інтелекту ЄС було ухвалено перший комплексний акт про штучний інтелект, яким упроваджується заборона на



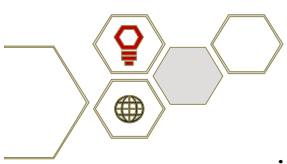
продукти з неприйнятним ризиком і посилюється регулювання додатків з високим ризиком [18].

У сфері кібербезпеки важливу роль відіграє Директива NIS2, яка замінила Директиву NIS1, розширивши обсяг регулювання та встановивши високі вимоги до держав-членів щодо створення стратегій кібербезпеки та захисту критичних секторів [19]. Директива також передбачає створення національних груп реагування на інциденти та Європейської мережі координації кіберкриз. Європейський Союз продовжує вдосконалювати чинне законодавство, зокрема шляхом перегляду Закону «Про кібербезпеку» (2019) з метою оптимізації процесів і зменшення адміністративного навантаження.

Стратегічні орієнтири цифрового розвитку ЄС. Важливою складовою цифрової політики Європейського Союзу є стратегія «Цифрове десятиліття» (2021), яка визначає цілі розвитку цифрових навичок населення, трансформації приватного сектору, розбудови безпечної цифрової інфраструктури та цифровізації публічних (у т. ч. адміністративних послуг), зокрема охорони здоров'я, освіти тощо [20]. Водночас, щорічні звіти Європейської комісії засвідчують певні труднощі у досягненні поставлених цілей. Зокрема, другий звіт акцентує на необхідності прискорення реформ і посилення координації зусиль держав-членів з метою подолання існуючих прогалин.

У безпосередньому зв'язку з вказаною вище стратегією перебуває й інший документ. Так, президенткою Європейської комісії Урсулою фон дер Ляєн у 2022 році було підписано Європейську декларацію цифрових прав та принципів. Цим документом Європейський Союз бере на себе зобов'язання щодо створення умов для безпечної, надійної та сталої цифрової трансформації, яка передбачає поєднання людиноцентристського підходу з основними цінностями Європейського Союзу та фундаментальними правами [21]. Декларація є тим документом, що визначає засади та орієнтири конкретної діяльності щодо втілення у життя програми «Цифрове десятиліття».

Як бачимо, Європейський Союз демонструє високу активність у сфері цифрової політики, поступово формуючи комплексну екосистему цифрового



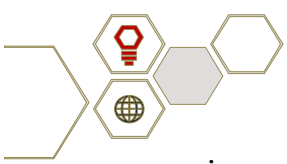
суверенітету. Незважаючи на значну кількість декларацій, стратегій, програм та інших актів, що формують політику ЄС, у цій сфері все ще достатньо викликів. Подальший успіх залежить від ефективності імплементації положень ухвалених актів, а також спроможності до адаптації до нових технологічних реалій.

Досвід Естонії у сфері цифрового суверенітету. Серед європейських держав Естонія має унікальний досвід у сфері цифрової трансформації. Одним із ключових досягнень, на наш погляд, є запровадження електронного голосування. У той час, коли інші країни лише планують або взагалі не розглядають таку можливість Естонія впевнено використовує електронне голосування з 2005 р.

З метою забезпечення належного функціонування системи електронного голосування (інтернет-голосування) необхідно було підготувати ґрунтовну нормативну основу. Так, спочатку виборець проходить автентифікацію відповідно до положень Закону «Про документи, що посвідчують особу» [22], який включає регулювання цифрового посвідчення особи, Регламенту ЄС «Про електронну ідентифікацію та довірчі послуги для здійснення електронних транзакцій» [23], а також Закону «Про захист персональних даних» [24]. Після успішного завершення процедури автентифікації сервер надає виборцю доступ до списку кандидатів відповідного виборчого округу.

Під час голосування виборець обирає кандидата, шифрує свій вибір із застосуванням випадкового шифрування відповідно до вимог Закону «Про кібербезпеку» [25]. Підписує криптограму цифровим підписом згідно із Законом «Про цифровий підпис» [26]. Після чого надсилає свій голос на сервер Vote Collector. Подальша передача даних здійснюється до спеціальної служби, яка засвідчує факт голосування за межами сервера та фіксує час надсилання. Для забезпечення прозорості процесу сервер Vote Collector надає виборцю підтвердження голосування у вигляді довідки, яку можна перевірити за допомогою мобільного пристрою через QR-код.

Як бачимо, Естонія створила надзвичайно складну та водночас надійну систему, яка мінімізує ризики фальсифікацій, завдяки високим технічним стандартам і якісному законодавчому врегулюванню. Як свідчать статистичні



дані, громадяни довіряють електронному голосуванню, а кількість користувачів системи постійно зростає [27].

Ще одним прикладом цифрової інновації є програма e-Residency, що була започаткована у 2014 р. [28]. Ця ініціатива полегшує ведення бізнесу, оскільки дозволяє підписувати документи в електронній формі з будь-якої точки світу за наявності інтернет-з'єднання та засобів електронної ідентифікації. Ця програма також суттєво спрощує відкриття бізнесу під юрисдикцією Естонії, усуваючи одну з головних проблем європейського бізнес-середовища – надмірну бюрократію. Користуватись програмою можуть навіть іноземні громадяни.

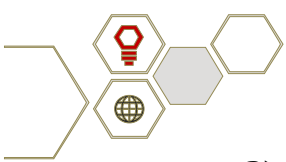
Відтак, завдячуючи комплексному підходу до правового регулювання та впровадженню сучасних технологій, Естонія досягла значних результатів у сфері цифрового суверенітету, ставши одним з лідерів серед європейських країн.

Проблеми формування власної моделі цифрового суверенітету України у воєнний час. У сучасних умовах, коли Україна перебуває у стані війни, питання цифрового суверенітету набуває особливої ваги. Захист персональних даних, забезпечення кібербезпеки, контроль за цифровою інфраструктурою та розвиток власних технологій, є не лише елементами економічної незалежності, а й важливими чинниками національної безпеки.

Досвід формування політики у сфері цифрового суверенітету Європейського Союзу, зокрема, й здобутки Естонії у цій сфері, демонструє, що побудова ефективної цифрової політики потребує комплексного підходу до регулювання різних аспектів цифрової сфери, розроблення якісної нормативної основи, зокрема, й стратегій довгострокового розвитку та програм їх втілення, а також постійного удосконалення законодавства, адаптацію до нових викликів.

На наш погляд, для України, з метою формування власної моделі цифрового суверенітету, вкрай важливими є такі комплексні заходи:

- 1) удосконалення чинного законодавства у сфері кібербезпеки, електронної ідентифікації, захисту даних, цифрових послуг;
- 2) розробити і ухвалити окремі законодавчі акти, спрямовані на захист критичної цифрової інфраструктури;



3) розробити стратегії цифрової трансформації / удосконалити існуючі на період повоєнного відновлення;

4) комплексно стимулювати розвиток національних технологічних компаній;

5) підтримувати і упроваджувати міжнародні ініціативи направлені на формування загальноєвропейської безпечної цифрової екосистеми.

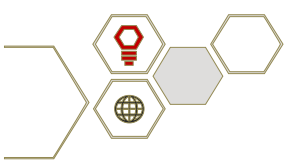
На особливу увагу заслуговує питання запровадження стандартів цифрового суверенітету у державному секторі, зокрема, щодо захисту інформаційних ресурсів, електронного урядування, електронного голосування, а також удосконалення системи електронних послуг для всіх категорій громадян.

Отже, шлях до цифрової незалежності України вимагає глибоких реформ, інвестицій у кібербезпеку, а також активної співпраці з надійними міжнародними партнерами.

Висновки. У результаті проведеного дослідження, метою якого було вивчити сучасний стан формування та розвитку моделі цифрового суверенітету в Європейському Союзі, дослідити успішний досвід цифрового розвитку Естонії та окреслити можливості його використання для України у воєнний час, було досягнуто поставлених цілей.

На основі аналізу нормативно-правових джерел та наукової літератури із використанням системного, формально-юридичного та формально-логічного методів наукового пізнання було з'ясовано, що цифровий суверенітет являє собою здатність держави забезпечувати контроль за цифровою інфраструктурою, захистом даних та цифровими сервісами. Дослідження свідчить, що ЄС послідовно розвиває нормативну базу у сфері цифрової безпеки та регулювання ринку, зокрема, шляхом ухвалення таких документів, як Регламент P2B, Закон «Про цифрові послуги» (DSA), Закон «Про цифрову операційну стійкість» (DORA), Закон «Про штучний інтелект» та Директива NIS2.

При цьому, особливий інтерес викликає досвід Естонії, яка першою в Європі запровадила електронне голосування, програму e-Residency, успішно



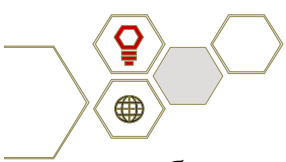
поєднавши розвинену цифрову інфраструктуру з відповідною законодавчою підтримкою. Метод порівняльно-правового аналізу дозволив виявити як сильні сторони європейських практик, так і ті аспекти, які залишаються невирішеними, зокрема, питання адаптивності законодавства до стрімких технологічних змін та забезпечення цифрової стійкості в умовах воєнних загроз. Для України, яка переживає збройну агресію з боку РФ, вивчення досвіду Європейського Союзу та Естонії зокрема, має особливе значення. Розвиток цифрового суверенітету є необхідною умовою для безпеки даних, сталого функціонування державних сервісів та економічної стійкості. У зв'язку з цим, існує нагальна потреба в удосконаленні чинного законодавства України, зокрема, за такими напрямками:

- 1) розроблення національної стратегії цифрового суверенітету;
- 2) посилення захисту критичної цифрової інфраструктури;
- 3) удосконалення регулювання діяльності платформ та цифрових послуг;
- 4) прийняття спеціальних актів щодо штучного інтелекту та кіберстійкості;
- 5) зменшення адміністративного навантаження та стимулювання подальшої цифрової трансформації бізнесу.

Таким чином, результати проведеного дослідження сприяють не лише розширенню теоретичних уявлень про цифровий суверенітет, а й формуванню конкретних напрямів державної політики України в умовах сучасних викликів за посередництвом практичних рекомендацій щодо подальших дій.

Список використаних джерел

1. Петришина М. О. Інноваційна складова муніципальної політики: проблеми та перспективи під час дії воєнного стану та у повоєнний період. Правове забезпечення науково-дослідницьких інфраструктур: зарубіжний досвід, тенденції та перспективи для України: кол .мон/ / за ред. А. М. Любич та І. В. Огієнко. Харків, НДІ ПЗІР НАПрНУ. 2023, 190 с. С. 86 – 119.
2. Єфремова К. В. Забезпечення цифрового суверенітету держави в умовах Індустрії 4.0. Конституційні засади розвитку інноваційного суспільства:



зб. наук. пр. за матер. інтернет-конфер., 25 червня 2021 року. Харків: НДІ ПЗІР НАПрНУ, 2021. С. 25 – 30.

3. Петришина М. О. Повноваження органів місцевого самоврядування у сфері створення належних організаційних та правових передумов розвитку дослідницьких структур в Україні. Правове забезпечення науково-дослідницької інфраструктури в Україні (теоретико-правовий аспект): кол. мон. / за ред. А. М. Любич та І. В. Огієнко. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2022. 176 с. С. 70 – 110.

4. Julia Pohle and Thorsten Thiel. Digital sovereignty, (2020). URL: <https://policyreview.info/concepts/digital-sovereignty>

5. Lucie Kadlecová. Cyber Sovereignty: The Future of Governance in Cyberspace. URL: https://www.youtube.com/watch?v=1MeszrYyMiE&ab_channel=TheHagueProgramonInternationalCyberSecurity

6. Renata Avila Pinto. Digital sovereignty or digital colonialism? URL: <https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/>

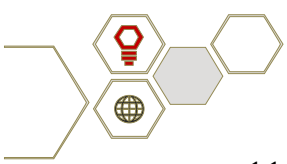
7. Stéphane Couture and Sophie Toupin. What does the notion of “sovereignty” mean when referring to the digital? (2019).

URL: https://www.researchgate.net/publication/335127008_What_does_the_notion_of_sovereignty_mean_when_referring_to_the_digital

8. Amsterdam Centre for European Studies. Preserving digital sovereignty of universities and researchers, (2023). URL: <https://aces.uva.nl/content/news/2023/11/preserving-digital-sovereignty-of-universities-and-researchers.html>

9. Digital Sovereignty and Citizens' Rights, (2021). URL: <https://europeanmovement.eu/policy/digital-sovereignty-and-citizens-rights-2/>

10. Sciences Po, «Цифровий суверенітет». URL: <https://www.sciencespo.fr/public/chaire-numerique/en/thematic-research/digital-and-data-sovereignty/>



11. World Economic Forum, 2025. URL:

<https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/>

12. Tietoevry. The path to digital sovereignty.

URL: <https://www.tietoevry.com/en/blog/2023/05/all-you-need-to-know-about-digital-sovereignty/>

13. Цифровий суверенітет Європи: від творця правил до супердержави в епоху суперництва між США та Китаєм.

URL: https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/#Artificial_intelligence:_Towards_a_pan-European_strategy

14. Регламент Європейського Парламенту та Ради про сприяння чесності та прозорості для бізнес-користувачів онлайн-посередницьких послуг. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018PC0238>

15. Закон «Про цифрові послуги».

URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

16. Politico. ЄС починає розслідування Temu.

URL: <https://www.politico.eu/article/eu-opens-probe-into-chinese-e-commerce-platform-temu/>

17. Закон «Про цифрову операційну стійкість».

URL: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en#:~:text=The%20Digital%20Operational%20Resilience%20Act,digital%20resilience%20of%20financial%20entities

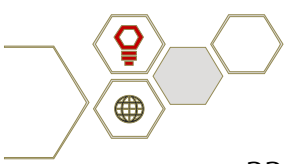
18. Закон «Про штучний інтелект». URL: <https://artificialintelligenceact.eu/>

19. Директива NIS2. URL:

<https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

20. Стратегія «Цифрове десятиліття Європи». URL: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>

21. Європейська декларація про цифрові права та принципи цифрового десятиліття. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001



22. Закон «Про документи, що посвідчують особу».

URL: <https://www.riigiteataja.ee/akt/126042024013>

23. Регламент ЄС «Про електронну ідентифікацію та довірчі послуги для здійснення електронних транзакцій».

URL: <https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng>

24. Закон «Про захист персональних даних».

URL: <https://www.riigiteataja.ee/akt/104012019011>

25. Закон «Про кібербезпеку».

URL: <https://www.riigiteataja.ee/akt/K%C3%BCTS>

26. Закон «Про цифровий підпис».

URL: <https://www.riigiteataja.ee/akt/694375>

27. Інтернет-голосування в Естонії 2005 – 2019.

URL: <https://www.sciencedirect.com/science/article/pii/S0740624X2200051X>

28. E-Residency. URL: <https://www.e-resident.gov.ee/>