

DOI: 10.34015/2523-4552.2025.2.03
УДК 342.8:004.9

Чалчинський В. І.,
аспірант Інституту держави і права
імені В. М. Корецького Національної
академії наук України
ORCID: 0009-0004-6318-4318

ЦИФРОВІЗАЦІЯ ВИБОРІВ: ПРОБЛЕМИ І ПЕРСПЕКТИВИ РОЗВИТКУ

Стаття присвячена аналізу проблем і перспектив впровадження цифрових технологій у виборчий процес, з акцентом на український контекст та міжнародний досвід. Досліджено сучасний стан цифровізації виборів, окреслено основні виклики, пов'язані з питаннями кібербезпеки, захисту персональних даних, рівня суспільної довіри та нормативного забезпечення. Запропоновано шляхи подолання цих проблем задля формування ефективної, безпечної та легітимної системи електронного голосування.

У статті розглядаються переваги цифровізації, зокрема підвищення доступності голосування для різних категорій громадян, скорочення адміністративних витрат, забезпечення прозорості підрахунку голосів за допомогою технологій блокчейн, а також зменшення впливу людського фактора. Водночас аналізуються серйозні ризики, такі як кіберзагрози, порушення конфіденційності даних, обмежена доступність цифрових платформ для певних груп населення та потенційні маніпуляції результатами. Особлива увага приділяється досвіду країн-піонерів, таких як Естонія, Швейцарія та Канада, де електронне голосування вже успішно застосовується, а також проблемним кейсам, як-от відмова Норвегії та Нідерландів від e-Voting через технічні та суспільні проблеми.

В українському контексті підкреслюється необхідність поетапного впровадження цифрових технологій, починаючи з пілотних муніципальних проєктів, із подальшим розширенням до національного рівня за умови вдосконалення кіберзахисту, правового регулювання та інституційної бази. Запропоновано синтетичну модель, яка поєднує технологічний прогрес із конституційними гарантіями, акцентуючи на важливості прозорої комунікації, незалежного аудиту та залучення громадськості для формування довіри до системи. Окремо наголошується на потребі кодифікації цифрових правовідносин у межах універсального «Цифрового кодексу» та адаптації до викликів майбутніх технологій, таких як квантові обчислення.

Підкреслено, що успіх цифровізації виборів залежить від синхронізації технологічних, правових і соціальних аспектів. Подальші дослідження мають зосередитися на розробці деталізованих процедур кіберзахисту, моделях електронної ідентифікації та стратегіях підвищення суспільної довіри до цифрових виборчих систем. Цифрові технології розглядаються як інструмент посилення демократії, що потребує чіткого правового регулювання та

орієнтації на принципи верховенства права, інклюзивності та захисту конституційних прав громадян.

Ключові слова: *цифровізація, цифровізація виборів, електронне голосування, кібербезпека, захист персональних даних, суспільна довіра, конституційні гарантії, блокчейн, правове регулювання, демократичні інститути, міжнародний досвід.*

Постановка проблеми. У сучасних умовах цифрової трансформації суспільства питання впровадження цифрових технологій у виборчий процес набуває особливої актуальності. Цифровізація виборів розглядається як один із ключових напрямів модернізації демократичних інституцій, що покликаний забезпечити більшу прозорість, оперативність, доступність і довіру до виборчих процедур. Водночас використання цифрових інструментів у виборчому процесі породжує низку складних проблем правового, технічного, організаційного та етичного характеру. Зокрема, постають питання гарантування кібербезпеки, захисту персональних даних, доступності електронного голосування для всіх категорій виборців, а також легітимності та надійності результатів голосування. Наявні моделі цифрового голосування, що впроваджуються у різних країнах, демонструють як певні успіхи, так і значні ризики, що потребують всебічного аналізу. Відповідно, дослідження проблем та перспектив цифровізації виборів є необхідним кроком для формування ефективної, безпечної та правово врегульованої системи електронного волевиявлення в демократичних державах.

Аналіз останніх досліджень і публікацій. Проблематиці цифровізації виборів, зокрема переваг та ризиків впровадження електронного голосування, кіберзахисту виборчих

процесів і конституційної відповідності цифрових інструментів участі, присвячено низку наукових та аналітичних досліджень. Зокрема, Є. Дуліба та В. Теремецький проаналізували зарубіжний досвід електронного голосування та визначили потенційні можливості для України в контексті демократичного розвитку [1]; Н. Черняшук акцентує на ролі фахівців із кіберзахисту в умовах сучасних викликів гібридної війни, зокрема щодо захисту цифрової інфраструктури виборчих систем [8]; у рішенні Федерального конституційного суду Німеччини, викладеному у публікації К. Шебс (K. Shebs), визначено правову позицію щодо неконституційності електронного голосування через порушення принципів прозорості та публічності виборчого процесу [11]. Утім, попри наявний доробок, залишається потреба в подальшому цілісному теоретико-правовому осмисленні цифрової трансформації виборчих процедур в умовах конституційної демократії.

Постановка завдання. Мета статті – дослідження сучасного стану цифровізації виборчого процесу, виявлення ключових проблем, що супроводжують впровадження цифрових технологій у сферу виборів, а також окреслення перспектив їх подальшого розвитку з урахуванням міжнародного досвіду та національних особливостей правового регулювання.

Виклад основного матеріалу.

Упродовж останніх двох десятиліть світова демократична спільнота інтенсивно інтегрує цифрові технології у процеси народного волевиявлення, трансформуючи класичні підходи до організації виборів та висуваючи на перший план конституційну вимогу забезпечення рівного, прямого й таємного голосування. Україна, перебуваючи в руслі глобального тренду, водночас потребує власної, зваженої відповіді на виклики кібербезпеки, захисту персональних даних та кризи суспільної довіри, аби повною мірою реалізувати потенціал, закладений у статтях 38, 69 і 71 Конституції [3].

Першопричиною інтересу до цифрового голосування виступає прагнення держав забезпечити більш широку, інклюзивну та оперативну участь громадян у демократичному процесі. У країнах-першопрохідцях, насамперед в Естонії, Швейцарії й Канаді, інтерактивні платформи для голосування через інтернет дозволили суттєво скоротити адміністративні витрати, підвищити явку молоді та громадян, які перебувають за кордоном, а також мінімізувати людський фактор під час підрахунку бюлетенів. Конфігурація цих систем демонструє, що технологічний ефект синергії досягається лише тоді, коли правові, організаційні та технічні механізми функціонують як єдине ціле. Український закон «Про Державний реєстр виборців» 2007 р. створив передумови для автоматизованого ведення списків, а Закон «Про електронну ідентифікацію та електронні довірчі послуги» 2017 р. імплементував інструмент Mobile ID, котрий може стати базовим компонентом автентифікації виборців у мережевому середовищі [4; 5]. Проте ці кроки залишаються фрагментарними: Виборчий кодекс, хоч і визнає можливість застосування цифрових технологій, поки що не пропонує достатньо деталізованих процедур, а отже, лише окреслює контури майбутньої реформи.

Переваги цифровізації у теоретичній площині виглядають переконливо. По-перше, знімається диспропорція між виборцями, які проживають у центрах та віддалених регіонах, що особливо актуально в умовах децентралізації та воєнного стану, коли логістика традиційних дільниць ускладнена. По-друге, забезпечується доступність для людей з інвалідністю, котрі часто зіштовхуються з бар'єрами фізичного середовища. По-третє, блокчейн-технології відкривають перспективу публічного, незмінного журналу транзакцій голосів, що підвищує прозорість підрахунку та знижує ймовірність фальсифікацій. Нарешті, зменшуються бюджетні витрати на друк бюлетенів, утримання дільничних комісій і транспортування документації, які традиційно становлять значну частку виборчого кошторису. Утім, перелічені аргументи мають сенс лише за реалізації низки передумов: від надійної системи ідентифікації до зрозумілих стандартів криптографічного захисту даних і сталих комунікаційних каналів між ЦВК, реєстрами й користувачами.

Ключовим ризиком вітчизняні дослідники вважають вразливість цифрових платформ до кіберзагроз. Так, Ю. Дуліба та В. Теремецький наголошують, що навіть у країнах із розвиненою ІТ-інфраструктурою існують прецеденти судових оскар-

жів. Крім того, впровадження нових технологій часто супроводжується проблемами з безпекою даних та приватністю виборців. Важливою складовою успішної реформи є також забезпечення високої прозорості процесу та надійності результатів. Це вимагає впровадження надійних механізмів моніторингу та аудиту, а також підвищення кваліфікації персоналу, який працює з електронними системами. Лише комплексний підхід, що враховує всі ці аспекти, може забезпечити справжню модернізацію виборчого процесу в Україні.

жень результатів електронного голосування через сумніви в цілісності даних, а в Україні – за рівня кіберзахисту, який лише формується, небезпека зовнішнього втручання багаторазово зростає [1]. До того ж естонський кейс, який часто позиціонують як зразковий, демонструє: стійкість системи не є сталою і потребує регулярного аудитування та оновлення сертифікатів безпеки. Водночас, відповідно до Закону «Про основні засади забезпечення кібербезпеки України», стратегічна модель протидії кібератакам має носити комплексний характер, але імплементація цих положень залишається фрагментарною [7]. Отже, без технічного вдосконалення «кіберщитів» і розбудови системи реагування на інциденти розгортати інтернет-голосування в загальнонаціональному масштабі передчасно.

Не менш чутливе питання – конфіденційність персональних даних і гарантія таємниці голосу. У західних юрисдикціях дедалі суворіші вимоги GDPR зумовили появу протоколів, що мінімізують збір даних про виборця та розділяють етап ідентифікації від етапу відправлення бюлетеня. В Україні правовий режим персональної інформації формально регулюється Законом «Про захист персональних даних» [6], однак практика показує, що досі недостатньо відпрацьовані процедури незалежного нагляду, відповідальності операторів і можливостей виборця оскаржити порушення. Скандал з Cambridge Analytica, який продемонстрував силу мікротаргетингу та маніпуляцій суспільними настроями, лише посилив підозри, що цифровий формат виборів може стати полігоном для витонченіших технологій

впливу [9]. Таким чином, запровадження інтернет-голосування без оновленої моделі захисту даних здатне трансформувати елемент демократії у інструмент прихованого контролю.

У науковому дискурсі щодо перспективності цифровізації виокремлюються дві домінантні позиції. Перша – «технологічного оптимізму» – спирається на аргументи економії ресурсів і зростання явки та пов'язана з іменами дослідників, які вивчають ефект інтернет-голосування у Естонії та Швейцарії. Є Дуліба й В. Теремецький, узагальнюючи ці дані, стверджують, що за правильно налаштованих процедур e-Voting підвищує рівень довіри до виборів, оскільки цифровий слід робить підрахунок прозорим, а доступ до інструментарію моніторингу отримує широкий спектр суб'єктів [1]. Друга позиція – «технологічного скепсису» – представлена фахівцями з кібербезпеки й конституційного права, які звертають увагу на асиметричність ризиків: одна успішна атака спроможна нівелювати роки еволюції демократичних інститутів [8]. Вони апелюють до прецедентів відмови Норвегії та Нідерландів від інтернет-голосування після виявлення технічних недоліків та низького рівня суспільної підтримки [10]. В українському контексті це означає слабкість інституційного забезпечення контролю за ланцюгом постачальників софту, ризики залучення іноземних хмарних сервісів та потенційну політизацію адміністратора ключів шифрування.

Порівняння обох підходів крізь призму конституційних гарантій дозволяє зробити висновок, що найбільш перспективною є синтетична

позиція, котра поєднує технологічний прогрес із інституційними запобіжниками. Усвідомлюючи реалії українського правового поля, доцільно розглядати «каскадну модель» запровадження цифрового голосування: від пілотних муніципальних проєктів – через добровільне дистанційне голосування для громадян, які проживають за кордоном – до поступового розширення масштабів у міру накопичення експертизи та довіри. Подібний підхід відповідає рекомендаціям Ради Європи щодо необхідності тестування систем у контрольованому середовищі та залучення багатосторонніх аудиторських команд. На користь такої стратегії свідчить і досвід Естонії: лише після серії успішних локальних виборів 2005 р. було ухвалено рішення про загальнонаціональне інтернет-голосування [2], причому акцент зроблено на безпаперовому аудиторському механізмі, що дозволяє виборцю переконатися у збереженні власного голосу без розкриття його змісту.

У контексті цього видається доцільним оновити нормативну архітектуру виборчого законодавства. У науковому середовищі дедалі частіше лунає пропозиція кодифікувати цифрові правовідносини у межах універсального «Цифрового кодексу», що містив би розділи про кібербезпеку, електронну ідентифікацію, порядок функціонування блокейн-реєстрів і, зокрема, моделі електронного голосування. Такий підхід сприяв би ліквідації колізій між галузевими актами та забезпечив би системність, якої сьогодні бракує точковим змінам. Окремої уваги потребує питання підзвітності постачальників програмного забез-

печення: ліцензування має бути доповнене вимогою відкритого коду, публічного аудиту та обов'язку збереження ключових компонентів серверної інфраструктури на території України. Лише за цих умов держава матиме юридичні та фактичні важелі для реагування на інциденти.

Особливого значення набуває проблема суспільної довіри. Як свідчить естонська та канадська практика, фактор «прозорості комунікації» відіграє не меншу роль, аніж технічна надійність. Систематичні інформаційні кампанії, залучення академічних експертів і громадських організацій до процедур стрес-тестування та демонстрацій голосування формують у виборця відчуття контролю й співучасті. Україна вже має позитивний досвід публічних презентацій реєстру виборців, однак цей формат слід якісно розширити: від інтерфейсних прототипів до симуляційних навчань для дільничних комісій, журналістів і представників політичних партій. Крім того, стратегія комунікації зобов'язана передбачити чіткий алгоритм оприлюднення результатів незалежного аудиту та відкриття даних, аби запобігти появі конспірологічних наративів.

Суттєвою перевагою поетапного підходу є можливість безболісно коригувати модель, спираючись на емпіричні дані пілотних проєктів. Наприклад, методологія «post-quantum readiness», що нині активно обговорюється у світовій криптографічній спільноті, передбачає поступову адаптацію алгоритмів шифрування до загроз майбутніх квантових комп'ютерів, а отже, пілоти можуть стати лабораторією для відпрацювання технік розподіленого шифрування та мультипідпису. Водночас

критики застерігають: надто тривала стадія тестових режимів ризикує цементувати «демократію двох швидкостей», коли окремі групи громадян отримують цифрові переваги, а інші продовжують користуватися застарілими процедурами. Подолати цю дихотомію можливо шляхом нормативного встановлення гарантованих термінів розгортання масштабних проектів і бюджетних зобов'язань держави.

У сфері конституційного контролю запровадження електронних виборів піднімає питання юрисдикції. Чи має Конституційний Суд отримати інструменти для ex-ante експертизи технічних протоколів? Чи слід передбачити спеціалізовані апеляційні колегії з питань кіберінцидентів у виборчому процесі? Іноземний досвід (наприклад, практика Федерального конституційного суду Німеччини щодо застосування електронних машин [11]) показує, що своєчасна конституційна фільтрація технологічних інновацій запобігає кризам легітимності. В українських реаліях важливо забезпечити механізм розмежування політичних і технічних суперечок, щоб уникнути сценарію, коли будь-які сумніви в працездатності цифрових систем використовуються як підстава для делегітимації результатів виборів.

У підсумку дискусії між «оптимістами» та «скептиками» вимальовується спільна точка згоди: невідворотність цифрової трансформації виборчих процедур. Різниця полягає у часових горизонтах і послідовності кроків. Еволюційний підхід, що зарекомендував себе в низці європейських юрисдикцій, видається придатним для України з огляду на потребу зміцнення кіберінфраструктури та

наращення кадрового потенціалу. Саме тому доцільною є позиція «синтетичного реалізму», згідно з якою розвиток електронного голосування має відбуватися одночасно на технологічному, правовому й суспільному рівнях, а оцінка результативності здійснюватися крізь призму конституційних цінностей, зокрема людської гідності, свободи й верховенства права.

Таким чином, цифровізація виборів у вітчизняному конституційно-правовому дискурсі – це багатогранний процес, у якому потенціал розширення прав громадян постійно взаємодіє з небезпекою технологічного вразливого місця. Вирішення зазначених проблем залежить від здатності держави синхронізувати правове регулювання з технічним прогресом, забезпечити прозорість алгоритмів і вибудувати культуру довіри, що базуватиметься на доказовій безпеці електронних систем та інклюзивності процесу прийняття рішень. Найперспективнішою є стратегія поступової імплементації e-Voting, інтегрованої у більш широку програму цифрового громадянства, яка поєднуватиме інновації з конституційними гарантіями та міжнародними стандартами демократичної легітимності.

Висновки. Цифровізація виборчого процесу в Україні є складним і багатогранним явищем, яке відкриває нові можливості для реалізації конституційних прав громадян, але водночас створює серйозні виклики, пов'язані з кібербезпекою, захистом даних та суспільною довірою. Найбільш перспективним є підхід, який передбачає поступове впровадження цифрових технологій через пілотні проекти, супроводжуване посилен-

ням правового регулювання та технічної інфраструктури. Успіх цифровізації можливий лише за умови комплексного підходу, який враховує як міжнародний досвід, так і національні особливості України. Важливо пам'ятати, що цифрові технології є лише інструментом, а не самоціллю, і їх використання має бути спрямоване на забезпечення принципів демократії, верховенства права та захисту конституційних прав громадян. У

цьому контексті необхідним є подальше дослідження правових, технічних та соціальних аспектів цифровізації виборів, а також активна співпраця між державою, громадянським суспільством та міжнародними організаціями для створення надійної та прозорої виборчої системи, яка відповідатиме викликам сучасності та забезпечуватиме реалізацію права громадян на вільне волевиявлення.

Список використаних джерел

1. Дуліба Є., Теремецький В. Переваги та ризики впровадження електронного голосування: досвід для України. *Актуальні проблеми правознавства*. 2024. № 1 (37). DOI:10.35774/app2024.01.078
2. Естонія проводить загальнонаціональне мережеве голосування. URL: https://archive.ph/20120713045721/http://news.com.com/Estonia+pulls+off+nationwide+Net+voting/2100-1028_3-5898115.html.
3. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. URL: <http://zakon2.rada.gov.ua/laws/show/254k/96-вр>.
4. Про Державний реєстр виборців : Закон України від 22.02.2007 р. № 698-V. URL: <https://zakon.rada.gov.ua/laws/show/698-16#Text>.
5. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII.
6. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481.
7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
8. Черняшук Н. Фахівці з кіберзахисту, чий рішення використовує Уряд України. Про «першу кібервійну у світі» та безпеку держпідприємств. URL: <https://lntu.edu.ua/uk/media/fakhivtsi-z-kiberzakhystu-chyyi-rishennya-vykorystovuye-uryad-ukrayiny-pro-pershu-kiberviynu>.
9. Cambridge Analytica, компанія в центрі скандалу з Facebook, закривається. URL: <https://www.bbc.com/ukrainian/news-43980978>.
10. E-voting experiments end in Norway amid security fears. URL: <https://www.bbc.com/news/technology-28055678>.
11. Shebs K. Germany high court finds electronic voting unconstitutional. URL: <https://www.jurist.org/news/2009/03/germany-high-court-rules-electronic/>.

Reference

1. Duliba Ye., Teremetskyi V. Advantages and risks of implementing electronic voting: experience for Ukraine. *Actual problems of jurisprudence*. 2024. № 1 (37). URL: <https://appj.wunu.edu.ua/index.php/appj/article/view/1812/1865>.
2. Estonia conducts nationwide online voting. URL: https://archive.ph/20120713045721/http://news.com.com/Estonia+pulls+off+nationwide+Net+voting/2100-1028_3-5898115.html.

3. Constitution of Ukraine : Law of Ukraine dated 28.06.1996 № 254к/96-VR. URL: <http://zakon2.rada.gov.ua/laws/show/254к/96-вр>.
4. On the State Register of Voters : Law of Ukraine dated 22.02.2007 № 698-V. URL: <https://zakon.rada.gov.ua/laws/show/698-16#Text>.
5. On electronic identification and electronic trust services : Law of Ukraine dated 05.10.2017 № 2155-VIII.
6. On personal data protection : Law of Ukraine dated 01.06.2010 № 2297-VI. Bulletin of the Verkhovna Rada of Ukraine. 2010. № 34. Art. 481.
7. On the basic principles of cybersecurity of Ukraine : Law of Ukraine dated 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
8. Cherniashchuk N. Cybersecurity specialists whose solutions are used by the Government of Ukraine. About the "first cyber war in the world" and the security of state enterprises. URL: <https://lntu.edu.ua/uk/media/fakhivtsi-z-kiberzakhyistu-chyyi-rishennya-vykorystovuye-uryad-ukrayiny-pro-pershu-kiberviynu>.
9. Cambridge Analytica, the company at the center of the Facebook scandal, is shutting down. URL: <https://www.bbc.com/ukrainian/news-43980978>.
10. E-voting experiments end in Norway amid security fears. URL: <https://www.bbc.com/news/technology-28055678>.
11. Shebs K. Germany high court finds electronic voting unconstitutional. URL: <https://www.jurist.org/news/2009/03/germany-high-court-rules-electronic/>.

Chalchynskyi Vladyslav, Ph.D student of the V. M. Koretsky Institute of State and Law research institute of the National Academy of Sciences of Ukraine
ORCID: 0009-0004-6318-4318

Digitalization of elections: challenges and development prospects

The article is devoted to the analysis of the problems and prospects of implementing digital technologies in the electoral process, with a focus on the Ukrainian context and international experience. It examines the current state of election digitalization and outlines key challenges related to cybersecurity, personal data protection, public trust, and regulatory frameworks. Solutions are proposed to overcome these issues and to build an effective, secure, and legitimate e-voting system.

The paper explores the advantages of digitalization, including increased accessibility of voting for various population groups, reduction of administrative costs, enhanced vote-counting transparency through blockchain technology, and minimization of human error. At the same time, it analyzes significant risks such as cyber threats, data confidentiality breaches, limited access to digital platforms for certain groups, and the potential for vote manipulation. Particular attention is given to the experience of pioneering countries like Estonia, Switzerland, and Canada, where e-voting is already successfully implemented, as well as problematic cases, such as the withdrawal of Norway and the Netherlands from e-voting due to technical and societal challenges.

In the Ukrainian context, the article emphasizes the need for a phased introduction of digital technologies, starting with pilot municipal projects and gradually expanding to the national level, provided that cybersecurity, legal regulation, and

institutional support are strengthened. A synthetic model is proposed that combines technological advancement with constitutional guarantees, highlighting the importance of transparent communication, independent auditing, and public engagement to foster trust in the system. Special attention is paid to the necessity of codifying digital legal relations within a universal «Digital Code» and preparing for future technological challenges such as quantum computing.

The article stresses that the success of election digitalization depends on synchronizing technological, legal, and social components. Future research should focus on developing detailed cybersecurity procedures, electronic identification models, and strategies to enhance public trust in digital electoral systems. Digital technologies are seen as tools to strengthen democracy, requiring clear legal regulation and adherence to the principles of the rule of law, inclusiveness, and the protection of constitutional rights.

Keywords: *digitalization, election digitalization, electronic voting, cybersecurity, personal data protection, public trust, constitutional guarantees, blockchain, legal regulation, democratic institutions, international experience.*