



Prospects of Post-War Voting in Ukraine: Issues of Introducing a State Internet Voting System in National Elections

UDC 342.82:004]:341.38(477)

DOI: <https://doi.org/10.15421/152627>

D4

Vorona Petro¹Dr.Sc., Full Prof., <https://orcid.org/0000-0002-6755-9023>, voron67@ukr.net**Frosiniak Ruslan²**Ph.D., Senior Lecturer, <https://orcid.org/0000-0002-5135-404X>, frosiniak@gmail.com**Khlaponin Dmytro³**Ph.D., Assoc. Prof., <https://orcid.org/0000-0002-7797-4319>, khlaponin_dy@knuba.edu.ua¹*Luhansk Taras Shevchenko National University (Poltava, Ukraine)*²*Donetsk State University of Internal Affairs (Kropyvnytskyi, Ukraine)*³*Kyiv National University of Construction and Architecture (Kyiv, Ukraine)*

Abstract.

The article examines the legal, technological, and security aspects of organizing the post-war electoral process in Ukraine within the context of the digitalization of public administration. It analyzes the destructive impact of Russian aggression on electoral infrastructure, large-scale internal and external population displacement, and the participation of a significant share of voters in the Defense Forces. Particular attention is paid to international experience with internet voting, especially Estonia, Switzerland, the United States, and Germany, as well as to end-to-end audit approaches and open architectures. The authors argue that a transition to full-scale remote internet voting in the immediate post-war elections would be premature because of high cybersecurity risks, threats of large-scale cyberattacks, constitutional requirements concerning ballot secrecy, and possible doubts about electoral legitimacy. The article identifies the main barriers to integrating internet technologies into Ukraine's electoral architecture and substantiates a hybrid approach to post-war electoral modernization. The transition toward smartphone-based voting should be gradual and based on phased digitalization, strong cybersecurity standards, auditable architectures, independent oversight, and sustainable public trust in digital state institutions.

Keywords: post-war elections, internet voting, public administration, cybersecurity, digital transformation, electoral infrastructure, international experience

Перспективи повоєнного волевиявлення в Україні: проблематика запровадження державної системи інтернет-голосування на національних виборах

Ворона Петро¹, Фросіняк Руслан², Хлапонін Дмитро³¹*Луганський національний університет імені Тараса Шевченка (Полтава, Україна)*²*Донецький державний університет внутрішніх справ (Кропивницький, Україна)*³*Київський національний університет будівництва і архітектури (Київ, Україна)*

Анотація.

У статті досліджено правові, технологічні та безпекові аспекти організації повоєнного виборчого процесу в Україні в контексті цифровізації публічного управління. Проаналізовано наслідки російської агресії для виборчої інфраструктури, масштабну зовнішню та внутрішню міграцію населення, а також перебування значної частини виборців у складі Сил оборони. Особливу увагу приділено міжнародному досвіду інтернет-голосування, зокрема практикам Естонії, Швейцарії, США та Німеччини, а також підходам до наскрізного аудиту відкритих архітектур. Обґрунтовано передчасність переходу до повноцінного дистанційного інтернет-голосування на найближчих повоєнних виборах через високі кібербезпекові ризики, загрози масштабних кібератак, конституційні вимоги щодо таємності волевиявлення та можливі сумніви щодо легітимності результатів. Виокремлено ключові бар'єри інтеграції інтернет-технологій у виборчу архітектуру України та обґрунтовано доцільність гібридного підходу. Перехід до «виборів у смартфоні» має бути поетапним і спиратися на високі стандарти кіберзахисту, відкриті для аудиту архітектури, незалежний контроль та стійку суспільну довіру.

Ключові слова: повоєнні вибори, інтернет-голосування, публічне управління, кібербезпека, цифрова трансформація, виборча інфраструктура, міжнародний досвід



Вступ.

Постановка проблеми.

Питання майбутнього розвитку України після завершення війни безпосередньо пов'язане з організацією та проведенням наступних виборів. Особливого значення набувають строки, умови та модель проведення виборчого процесу, оскільки від них значною мірою залежатиме подальша стабільність демократичних інститутів держави.

В умовах воєнного стану проведення виборів Президента України, Верховної Ради України та органів місцевого самоврядування законодавством заборонено. Відповідне положення передбачене статтею 19 Закону України «Про правовий режим воєнного стану» (Закон України № 389-VIII, 2015). Водночас конституційно-правове регулювання передбачає безперервність функціонування органів державної влади, а повноваження відповідних суб'єктів продовжуються до моменту набуття повноважень новообраними представниками у встановленому законом порядку (Конституція України, 1996). Таким чином, після припинення воєнного стану Україна може зіткнутися із серйозним випробуванням спроможності демократичної системи забезпечити легітимний, інклюзивний та безпечний виборчий процес. При цьому проведення виборів може бути актуальним не лише після остаточного завершення збройної агресії, а й у разі припинення активної фази бойових дій за умови досягнення необхідного рівня безпеки.

Проведення повоєнних виборів потребуватиме належної підготовки та, ймовірно, внесення спеціальних змін до виборчого законодавства. Необхідність такого підходу зумовлена масштабними соціальними та демографічними змінами, спричиненими війною. Значна кількість громадян України перебуває у складі Сил оборони, мільйони людей стали внутрішньо переміщеними особами або тимчасово проживають за кордоном. Частина громадян перебуває за межами своїх територіальних громад, що ускладнює застосування традиційних механізмів організації голосування.

Додатковою проблемою є масштабне пошкодження та знищення цивільної інфраструктури. Внаслідок бойових дій були зруйновані або пошкоджені заклади освіти, культури, охорони здоров'я, адміністративні будівлі та інші об'єкти, які традиційно використовувалися для розміщення виборчих дільниць.

Отже, відновлення виборчої інфраструктури

також стане важливою складовою підготовки до повоєнних виборів.

Проблематика організації виборчого процесу після завершення війни набуває дедалі більшого значення, оскільки результати майбутніх виборів можуть істотно вплинути на формування політичного ландшафту України, склад парламенту, органів виконавчої влади та місцевого самоврядування. Водночас характер майбутньої виборчої системи матиме безпосередній вплив на процес відновлення держави, соціально-економічний розвиток та зміцнення демократичних інститутів.

Сучасні наукові та експертні дискусії щодо повоєнного виборчого процесу в Україні можна умовно поділити на три основні напрями:

- визначення юридичної та політичної доцільності проведення виборів в умовах збройного конфлікту або безпосередньо після його завершення;
- оцінювання можливостей застосування електронного та дистанційного інтернет-голосування як додаткового механізму залучення військовослужбовців, внутрішньо переміщених осіб та громадян України, які проживають за кордоном;
- адаптація традиційних виборчих систем, територіальної організації виборів та виборчих округів до масштабних міграційних процесів і зміни структури населення.

До обговорення зазначених питань залучені представники різних наукових і професійних сфер: фахівці з державного управління, політологи, соціологи, правники, військові аналітики, спеціалісти з інформаційних технологій та практики публічного управління. Такий міждисциплінарний характер дискусії дає змогу розглядати проблему не лише з позиції виборчого права, а й комплексно – з урахуванням безпекових, технологічних, соціальних та управлінських чинників (Кабінет Міністрів України, n.d.). Комплексне дослідження зазначених аспектів є необхідним для формування цілісної моделі відновлення демократичного процесу в Україні та мінімізації ризиків виникнення політичних і соціальних конфліктів у повоєнний період.

Метою статті є комплексний аналіз перспектив організації повоєнного виборчого процесу в Україні, зокрема визначення основних проблем і технологічних бар'єрів, пов'язаних із можливим запровадженням державної системи дистанційного інтернет-голосування на національних виборах.

Окрему увагу приділено питанням безпеки,



прозорості, анонімності та можливості незалежної перевірки результатів електронного голосування. Важливим аспектом є також забезпечення довіри громадян до відповідної системи, особливо з огляду на необхідність протидії корупційним ризикам, кібератакам та можливому втручання у виборчий процес. Потенційною технологічною основою для розвитку таких механізмів може стати наявна цифрова інфраструктура держави, зокрема мобільний застосунок та вебпортал «Дія», розроблені Міністерством цифрової трансформації України (Мазур, 2020). Водночас наявність технологічної бази сама по собі не гарантує суспільної довіри. Тому запровадження електронного голосування має супроводжуватися незалежним аудитом, відкритістю програмного забезпечення, належним правовим регулюванням та дієвими механізмами громадського і міжнародного контролю.

Аналіз попередніх досліджень і публікацій.

Одним із важливих напрямів розвитку електронного голосування є забезпечення прозорості програмного забезпечення та можливості його незалежного аудиту. Американський дослідник Брюс Шнайер у своїх працях (Schneier, 2004, 2020) наголошував на проблемах використання закритого програмного забезпечення у виборчих системах та необхідності забезпечення можливості незалежної перевірки технологічних рішень.

На думку дослідника, безпека виборчих технологій не повинна ґрунтуватися виключно на секретності програмного забезпечення. Навпаки, відкритість коду та можливість його перевірки незалежними експертами можуть сприяти виявленню вразливостей і підвищенню довіри до системи. Такий підхід передбачає розроблення максимально простих і зрозумілих технологічних рішень, які можуть бути піддані незалежному аудиту.

Проблематику побудови системи таємного електронного голосування через публічну мережу інтернет досліджував доктор технічних наук Юрій Хлапонін. У своїх працях він розглядає можливості проведення аудиту програмного та апаратного забезпечення, а також окремих процедур, які можуть впливати на довіру виборців до результатів голосування (Khlaponin et al., 2020). Відкритість технологічних процесів та можливість їх незалежної перевірки розглядаються як важливі умови підвищення надійності системи.

Олександр Мазур досліджував тенденції

розвитку електронного урядування в органах публічного управління різних держав на основі аналізу міжнародних наукових публікацій (Мазур, 2020). Отримані результати дають змогу розглядати цифровізацію державного управління як ширший процес, у межах якого електронне голосування може виступати одним із напрямів подальшого розвитку цифрових публічних послуг.

Міжнародна практика електронного голосування демонструє поступовий перехід від використання електронних виборчих машин безпосередньо на виборчих дільницях до дистанційних моделей голосування через інтернет. Найбільш відомим прикладом системного використання дистанційного електронного голосування є Естонія. Водночас окремі моделі електронного голосування застосовувалися або тестувалися у Швейцарії, США, Франції та інших державах. Частина країн відмовилася від окремих технологічних рішень через виявлені ризики безпеки (Гринов & Закоморна, 2021; Гусаревич, 2022; Лісовський, 2023; Панкратов, 2023).

Роман Була розглядає електронне голосування як один із напрямів модернізації виборчого процесу. У його дослідженнях аналізується досвід Естонії, Швейцарії, Німеччини та США, а серед потенційних переваг електронного голосування визначаються підвищення доступності виборів, зручність участі, скорочення витрат, зменшення кількості технічних помилок та пришвидшення обробки результатів. Водночас автор звертає увагу на кібербезпекові ризики, цифрову нерівність та проблему довіри громадян до нових технологій (Була, 2025).

Питання демократії та залучення громадян до формування державної політики із застосуванням інформаційно-комунікаційних технологій досліджували Ч. Армстронг, Ю. Гарлан, С. Коулман та інші науковці. Проблематика електронного голосування і можливостей його застосування в Україні представлена у працях М. Афанасьєвої, О. Бойко, М. Бучина, Н. Грицяк, Ю. Ключковського, О. Радченка та інших дослідників.

Виклад основного матеріалу.

Виборча система України передбачає проведення загальнодержавних і місцевих виборів. До загальнодержавних належать вибори Президента України та народних депутатів України, тоді як на місцевому рівні обираються представники органів місцевого самоврядування, зокрема голови та депутати відповідних рад.

Одним із можливих напрямів модернізації виборчого процесу є використання електронного голосування (ЕГ). Основні європейські підходи до його організації визначені Рекомендацією Комітету міністрів Ради Європи Rec(2004)11 від 30 вересня 2004 року «Щодо правових, операційних та технічних стандартів електронного голосування» (Council of Europe, 2004).

Відповідно до положень Рекомендації, застосування електронного голосування може сприяти розширенню доступу громадян до виборчого процесу, зокрема тих осіб, які перебувають за межами місця свого постійного проживання або за кордоном. Технологічні рішення також можуть полегшити участь людей з інвалідністю та інших громадян, для яких фізичне відвідування виборчої дільниці є складним. Серед потенційних переваг електронного голосування також можна виокремити розширення каналів участі у виборах, скорочення організаційних витрат у довгостроковій перспективі, прискорення обробки результатів та підвищення зручності для виборців (Council of Europe, 2004).

Водночас застосування електронних технологій не повинно призводити до обмеження фундаментальних принципів виборчого права. Система має забезпечувати загальність, рівність, свободу та таємність голосування, а також передбачати відповідні процедурні гарантії. Інтерфейс електронної системи повинен бути зрозумілим і доступним для користувачів. Особливу увагу необхідно приділяти виборцям з інвалідністю та громадянам, які мають недостатній рівень цифрової грамотності. Крім того, у разі неможливості забезпечити рівний доступ усіх виборців до дистанційного електронного голосування воно не повинно ставати єдиним способом реалізації виборчого права (Council of Europe, 2004).

Важливою умовою є також недопущення повторного врахування одного голосу у випадку використання різних каналів голосування. Виборець повинен мати можливість контролювати власне рішення в межах встановленої процедури, а система не повинна створювати умов для маніпулятивного впливу на нього.

Особливе значення має гарантування таємниці голосування. Жоден етап процедури – від ідентифікації виборця до обробки та підрахунку голосів – не повинен створювати можливості встановити відповідність між конкретним виборцем і його вибором (Council of Europe, 2004).

Не менш важливим є незалежний контроль за функціонуванням системи. До її запровадження, а також після внесення істотних змін має здійснюватися незалежна перевірка програмного забезпечення, технічної інфраструктури, засобів захисту інформації та можливості достовірного встановлення результатів голосування (Council of Europe, 2004).

На практиці електронні технології можуть використовуватися у різних формах. Серед них – системи оптичного сканування паперових бюлетенів, технології прямого електронного запису голосу, електронні пристрої для голосування та автоматизовані системи підрахунку результатів. Відповідні технології застосовуються у різних державах, зокрема в Австралії, Бельгії, Великій Британії, Бразилії, США та на Філіппінах (Романенко, 2019). Окрему групу становлять дистанційні системи інтернет-голосування, які дозволяють виборцю здійснювати волевиявлення за допомогою персонального комп'ютера, планшета або мобільного телефону. Такі технології використовувалися або тестувалися, зокрема, в Естонії, Швейцарії, Великій Британії, Канаді та інших державах (Панкратов, 2023, с. 56–57).

Електронні виборчі машини (EVM – Electronic Voting Machines) є комп'ютеризованими пристроями, призначеними для автоматизації окремих етапів виборчого процесу, зокрема реєстрації виборців, безпосереднього голосування або підрахунку голосів (Кабінет Міністрів України, n.d.). Їх застосування має на меті скорочення часу обробки результатів та зменшення кількості помилок, пов'язаних із ручним підрахунком паперових бюлетенів (Encyclopaedia Britannica, n.d.). До основних технологічних моделей можна віднести:

- системи прямого електронного запису (DRE – Direct-Recording Electronic) – виборець здійснює вибір за допомогою сенсорного екрана, кнопок або іншого електронного інтерфейсу, після чого інформація фіксується в пам'яті пристрою;

- оптичні сканери бюлетенів – виборець заповнює паперовий бюлетень, який після цього сканується спеціальним пристроєм, а результати автоматично обробляються;

- пристрої маркування бюлетенів (BMD – Ballot Marking Devices) – технологічні засоби, що дають змогу виборцю сформувати паперовий бюлетень за допомогою електронного інтерфейсу, зокрема з використанням аудіосупроводу чи інших спеціальних функцій доступності (Encyclopaedia Britannica, n.d.).



Альтернативою зазначеним технологіям є дистанційне інтернет-голосування. Його принципова відмінність полягає в тому, що виборець не повинен фізично перебувати на виборчій ділянці. Ідентифікація може здійснюватися за допомогою електронного документа, ID-картки, спеціальної смарт-картки, електронного підпису або інших засобів цифрової автентифікації.

Досвід різних країн свідчить, що технологічні моделі електронного голосування суттєво відрізняються. Наприклад, в Естонії цифрова ідентифікація громадян використовується не лише для участі у виборах, а й для отримання широкого спектра державних та приватних електронних послуг (Гринов & Закоморна, 2021).

Для України особливо актуальним є питання можливого використання вже сформованої цифрової інфраструктури. Зокрема, мобільний застосунок «Дія» та відповідний вебпортал стали важливими елементами цифрової взаємодії громадян із державою (Українська правда, 2023; Вишняков та ін., 2014). Значна кількість користувачів цієї інфраструктури створює технологічне підґрунтя для дискусії щодо можливості її використання в майбутньому для реалізації окремих виборчих процедур.

Водночас поширеність цифрових державних сервісів не може автоматично означати готовність суспільства до дистанційного голосування. Виборча система має відповідати значно вищим вимогам щодо безпеки, анонімності, прозорості та перевірюваності, ніж звичайні електронні державні послуги.

Саме тому для України важливо детально дослідити міжнародний досвід, зокрема практику Естонії та Швейцарії, а також проаналізувати технологічні й правові ризики.

Досвід Естонії. Одним із найбільш відомих прикладів використання інтернет-голосування є Естонія. На початку 2000-х років у країні було сформовано нормативно-правову основу для електронного голосування, яка включала положення законів про вибори до органів місцевого самоврядування, парламенту, Європейського парламенту та проведення референдумів (Топалова, 2020).

Важливою передумовою стало створення розвиненої системи цифрової ідентифікації. Електронна ID-картка дозволила громадянам користуватися цифровим підписом і широким спектром електронних державних та приватних послуг, включно з дистанційним голосуванням (Гринов & Закоморна, 2021).

Перший практичний досвід інтернет-

-голосування було отримано під час місцевих виборів 2005 року. Надалі система використовувалася під час парламентських, європейських та інших виборів.

За наведеними у дослідженнях даними, на парламентських виборах 2023 року дистанційним способом проголосували понад 300 тисяч виборців, що становило більше половини всіх учасників голосування (Solvak & Vassil, 2018). Цей результат демонструє значний рівень поширення електронного способу голосування серед естонських громадян. До основних елементів естонської моделі належать електронна ідентифікація, криптографічний захист інформації та можливість перевірки виборцем факту коректного врахування його волевиявлення.

Водночас тривалий досвід Естонії не означає відсутності ризиків. Система постійно перебуває під загрозою кібератак і потребує регулярного оновлення засобів захисту. Окремим фактором залишається суспільна довіра: будь-які повідомлення про можливі маніпуляції здатні створювати політичну напругу та ставити під сумнів легітимність результатів (Радіо Свобода, 2009).

Для України ця проблема може бути ще більш гострою через масштабні безпекові загрози, активність російських кібероперацій та високі суспільні вимоги до прозорості виборів. Тому потенційна українська система інтернет-голосування повинна поєднувати технічний захист, незалежний аудит, відкритість процедур та можливість зовнішнього контролю. Особливо важливо забезпечити одночасне виконання двох принципово різних вимог: неможливість встановлення вибору конкретного виборця та можливість перевірки коректності функціонування системи.

Необхідно також передбачити ефективні механізми протидії примусу та підкупу виборців. У разі запровадження дистанційного голосування відповідні норми мають бути належним чином узгоджені з виборчим і кримінальним законодавством.

Технологічні механізми захисту інтернет-голосування. Для мінімізації ризиків електронного голосування можуть застосовуватися різні технологічні та організаційні механізми.

1. Надійна ідентифікація та автентифікація виборців. Система повинна забезпечувати однозначне встановлення особи виборця. Для цього можуть використовуватися кваліфікований електронний підпис, багатфакторна

автентифікація, державні системи цифрової ідентифікації та інші захищені механізми.

2. Криптографічний захист інформації. Застосування сучасних криптографічних протоколів має забезпечувати конфіденційність вибору та унеможливлювати несанкціоноване втручання у процес обробки голосів. Серед потенційних технологій розглядаються сліпі підписи та гомоморфне шифрування.

3. Наскрізна перевірюваність. Виборець повинен мати можливість переконатися, що його волевиявлення було належним чином прийняте системою та включене до процедури підрахунку, не розкриваючи при цьому зміст свого голосу третім особам.

4. Захист від примусу та підкупу. Одним із можливих механізмів є надання виборцю права повторно здійснити волевиявлення протягом установленого періоду, при цьому чинним визнається останній голос. Такий підхід потенційно зменшує ризик ситуацій, коли особа змушена голосувати під контролем іншої людини.

5. Відкритий код та незалежний аудит. Програмне забезпечення виборчої системи має бути доступним для незалежної перевірки. До аудиту доцільно залучати фахівців із кібербезпеки, представників наукової спільноти, міжнародних експертів та громадянського суспільства. Перед запуском системи необхідно проводити масштабне тестування її захищеності (Була, 2025; Гринов & Закоморна, 2021; Гусаревич, 2022; Мазур, 2020; Панкратов, 2023; Романенко, 2019; Khlaponin et al., 2020).

Досвід Швейцарії. Іншим важливим прикладом є Швейцарія, де електронне голосування розвивається переважно на кантональному рівні, що відповідає федеративній структурі держави. Пілотні проекти були започатковані у 2003 році, а згодом окремі кантони почали використовувати електронне голосування для визначених категорій виборців, зокрема громадян, які проживають за кордоном.

Швейцарська модель передбачає використання засобів електронної ідентифікації та захищеного передавання виборчого волевиявлення. Важливою особливістю є можливість дострокового дистанційного голосування та зміни свого рішення до завершення встановленого періоду голосування (Лісовський, 2023).

Досвід Швейцарії демонструє, що впровадження електронного голосування може здійснюватися поступово – через пілотні проекти, обмеження кола виборців та постійне тестування технологічних рішень.

Основні загрози запровадження інтернет-голосування в Україні

В українських умовах ризики дистанційного голосування доцільно розглядати за кількома основними напрямками.

1. Кіберзагрози та воєнний фактор.

Українська виборча інфраструктура потенційно може стати однією з ключових цілей кібератак з боку Російської Федерації. Серед можливих загроз – DDoS-атаки, несанкціонований доступ до інформаційних систем, викрадення даних, спроби втручання у програмне забезпечення та маніпулювання результатами (Була, 2025).

Окремою проблемою є безпека пристроїв самих виборців. Навіть захищена центральна інфраструктура не усуває ризик використання шкідливого програмного забезпечення на персональних комп'ютерах або смартфонах.

2. Ризики порушення фундаментальних принципів виборчого права.

Найскладнішою проблемою дистанційного голосування залишається забезпечення таємниці волевиявлення. На відміну від контрольованої виборчої дільниці, держава не може повною мірою контролювати умови, у яких громадянин голосує вдома або в іншому місці.

Це створює ризики сімейного чи адміністративного примусу, а також підкупу виборців. Наприклад, стороння особа може вимагати від виборця продемонструвати процес голосування або надати інші докази зробленого вибору.

3. Технічні та процедурні проблеми.

Паперовий бюлетень створює фізичний слід, який у разі необхідності може бути повторно перевірений. В електронній системі значна частина процесів відбувається у цифровому середовищі, тому незалежному спостерігачеві без спеціальних технічних знань складніше самостійно оцінити коректність роботи системи. Додатковий ризик пов'язаний з ідентифікацією користувача. Необхідно виключити можливість використання сторонніми особами електронних підписів, облікових записів або інших засобів цифрової ідентифікації.

4. Соціальна та політична недовіра.

Навіть технічно безпечна система може виявитися недостатньо ефективною, якщо значна частина суспільства не довірятиме її результатам. Будь-який масштабний технічний збій, інформаційна атака або повідомлення про можливе втручання можуть стати підставою для сумнівів у легітимності виборів (Радіо Свобода, 2009). Окремим викликом залишається цифрова



нерівність. Не всі громадяни мають однаковий рівень доступу до швидкісного інтернету, сучасних пристроїв та цифрових навичок. Особливо актуальною ця проблема може бути для мешканців сільських територій, прифронтових районів та громадян старшого віку.

Порівняння переваг і ризиків. З огляду на українські реалії переваги та ризики інтернет-голосування доцільно оцінювати щонайменше за чотирима критеріями: доступністю, кібербезпекою, таємністю голосування та довірою до результатів.

Доступність. Дистанційне голосування потенційно може суттєво спростити участь у виборах для громадян, які перебувають за кордоном або є внутрішньо переміщеними особами. Водночас технологія не усуває проблеми відсутності електроенергії, інтернету чи відповідного пристрою, особливо на територіях, що постраждали від бойових дій.

Кібербезпека. Україна має значний досвід розвитку цифрових державних сервісів та протидії кіберзагрозам. Однак саме виборча система може стати особливо привабливою цілью для масштабних атак, оскільки її компрометація може мати не лише технічні, а й серйозні політичні наслідки.

Таємність голосування. Дистанційне голосування створює ризик контролю виборця з боку членів сім'ї, роботодавців, представників незаконних формувань або інших осіб. Одночасно воно забезпечує значно більшу фізичну доступність процесу, оскільки громадянин може брати участь у виборах без відвідування виборчої дільниці.

Довіра до результатів. Автоматизований підрахунок може суттєво скоротити час встановлення результатів. Проте відсутність традиційного паперового сліду може ускладнювати незалежну перевірку та фізичний перерахунок, що за певних обставин здатне посилити суспільні сумніви щодо достовірності результатів.

Таким чином, електронне голосування не може розглядатися виключно як технологічна альтернатива традиційним виборам. Його потенційне впровадження в Україні потребує одночасного вирішення правових, організаційних, соціальних та кібербезпекових питань.

У повоєнних умовах найбільш доцільним може бути поступовий підхід, за якого електронне голосування спочатку тестується у контрольованих умовах, проходить незалежний аудит та оцінюється з точки зору впливу на виборчі права громадян. Лише після

підтвердження його безпечності, надійності та суспільної прийнятності може розглядатися питання масштабного застосування.

Ключовою умовою при цьому має залишатися не технологічна новизна системи, а її здатність забезпечити чесність виборів, таємницю волевиявлення, рівність громадян та довіру до встановлених результатів.

Висновки.

На основі проведеного комплексного аналізу перспектив та викликів упровадження цифрових технологій у виборчий процес України у повоєнний період можна сформулювати такі висновки:

1. *Встановлено передчасність переходу на повноцінне дистанційне інтернет-голосування на найближчих післявоєнних виборах в Україні.* Попри очевидну технологічну привабливість, такий крок наразі є неможливим і недоцільним через критично високі безпекові ризики, загрози масштабних кібератак та потенційні сумніви щодо легітимності результатів волевиявлення. Сучасні міжнародні інституції, зокрема Рада Європи, рекомендують розглядати е-голосування виключно як стратегічну перспективу віддаленого майбутнього.

2. *Систематизовано ключові виклики та бар'єри на шляху інтеграції інтернет-технологій у виборчу архітектуру України:*

- *Фактор воєнної агресії РФ.* Жодна з існуючих у світі цифрових виборчих систем не здатна гарантувати 100% імунітет від цільових, високотехнологічних кібератак з боку країни-агресора, яка володіє потужним потенціалом кібервійни.

- *Конституційно-правові обмеження.* Конституція України імперативно гарантує таємність та прямий характер голосування. У випадку дистанційного інтернет-волевиявлення держава позбавлена можливості технічного чи процедурного контролю за тим, чи здійснювався зовнішній примус або тиск на виборця в момент безпосередньої авторизації та натискання кнопки на персональному пристрої.

- *Обмеженість світового досвіду.* Єдиним повністю успішним кейсом тотального онлайн-голосування на національному рівні залишається Естонія, яка вибудовувала суспільну довіру та цифрову інфраструктуру десятиліттями і не перебуває у стані гарячої війни. Натомість провідні європейські демократії (Франція, Німеччина, Нідерланди) свого часу офіційно відмовилися від електронних виборів через неможливість гарантувати абсолютну безпеку підрахунку голосів.



3. Обґрунтовано раціональність упровадження гібридного підходу для модернізації повоєнного виборчого процесу в Україні. Перехід до «виборів у смартфоні» має відбуватися еволюційно, шляхом поетапної цифровізації окремих елементів:

- Наскрізна модернізація Державного реєстру виборців (ДРВ);
- Запровадження онлайн-запису на дільниці (зокрема для оптимізації черг у закордонних дипломатичних установах);

- Використання сучасних електронних сканерів бюлетенів на класичних дільницях для автоматизації та прискорення підрахунку голосів.

Повноцінне дистанційне інтернет-голосування на національному рівні в Україні може стати реальністю лише в довгостроковій перспективі після повного завершення війни, досягнення найвищих стандартів кіберзахисту, впровадження відкритих для аудиту архітектур та формування стійкої суспільної довіри громадян до цифрових інститутів держави.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

- Була, Р. (2025). Світовий досвід е-виборів та е-голосування: перспективи та досвід для України. *Вісник Львівського університету. Серія філософсько-політологічні студії*, 58, 242–250. <https://doi.org/10.30970/PPS.2025.58.30>
- Вишняков, В. М., Пригара, М. П., & Воронін, О. В. (2014). Відкрита система таємного голосування. *Управління розвитком складних систем*, 20, 110–115.
- Ворона, П. В., Гошовська, В. А., & Лопушинський, І. П. (2016). *Місцева влада в країнах пострадянського простору*. ПП Шевченко.
- Гринов, С. О., & Закоморна, К. О. (2021). Електронне голосування: перспективи впровадження в Україні та зарубіжний досвід. *Юридичний науковий електронний журнал*, 4, 101–105. <https://doi.org/10.32782/2524-0374/2021-4/23>
- Гусаревич, Н. (2022). Технологічні рішення щодо забезпечення електронного голосування у виборчому процесі: закордонний досвід. *Аспекти публічного управління*, 10(1), 26–35. <https://doi.org/10.15421/152273>
- Кабінет Міністрів України. (n.d.). *Операція «електронізація». Електронне голосування і підрахунок*. <https://petition.kmu.gov.ua/petitions/2159>
- Конституція України: Закон України № 254к/96-ВР. (1996). *Відомості Верховної Ради України*, 30, ст. 141. <https://zakon.rada.gov.ua/laws/show/254k/96-vr#Text>
- Лісовський, Ю. (2023, 7 листопада). Інтернет-голосування та шкідливе програмне забезпечення: приклад Швейцарії. *Громадянська мережа ОПОРА*. <https://www.oporaua.org/vybory/internet-golosuvannya-ta-shkidlivoprogramne-zabezpechennya-priklad-shveycariyi-24995>
- Мазур, О. (2020). Сучасні тенденції упровадження електронного урядування в публічному управлінні: зарубіжний досвід. *Аспекти публічного управління*, 7(12), 147–156. <https://doi.org/10.15421/151974>
- Панкратов, В. (2023). Електронне голосування як елемент електронної демократії: досвід країн ЄС. *Науковий вісник Ужгородського національного університету. Серія: Право*. <http://journal-app.uzhnu.edu.ua/article/view/294405/287190>
- Про правовий режим воєнного стану: Закон України № 389-VIII. (2015). *Відомості Верховної Ради України*, 28, ст. 250. <https://zakon.rada.gov.ua/laws/show/389-19#Text>
- Радіо Свобода. (2009, 3 березня). *У Німеччині заборонили електронне голосування на виборах*. <https://www.radiosvoboda.org/a/1503517.html>
- Романенко, Є. О. (2019). Електронне голосування – шлях до впровадження електронних механізмів демократії в Україні. *Публічне урядування*, 4(19), 259–271. [https://doi.org/10.32689/2617-2224-2019-4\(19\)-259-271](https://doi.org/10.32689/2617-2224-2019-4(19)-259-271)
- Топалова, С. (2020, 30 квітня). Запуск електронного голосування: корисний досвід Естонії. *LB.ua*. https://lb.ua/blog/svetlana_topalova/456467_zapusk_elektronного_golosuvannya.html
- Українська правда. (2023, 6 березня). *Вибори в Естонії: вперше в історії понад 50% виборців голосували онлайн*. <https://www.eurointegration.com.ua/news/2023/03/6/7157420/>
- Council of Europe, Committee of Ministers. (2004, September 30). *Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*.
- Electronic voting in Estonia. (n.d.). In *Wikipedia*. https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia
- Encyclopaedia Britannica. (n.d.). *Voting machines*. <https://www.britannica.com/procon/voting-machines-debate>
- Khlaponin, Y., Vyshniakov, V., Prygara, M., & Poltorak, V. (2020). The new concept of guaranteeing confidence in the e-voting system. In *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)* (pp. 747–752). IEEE. <https://doi.org/10.1109/PICST51311.2020.9468012>
- Schneier, B. (2004, November 1). *What's wrong with electronic voting machines?* Schneier on Security. https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html
- Schneier, B. (2020, March 15). *Voatz Internet voting app is insecure*. Schneier on Security. <https://www.schneier.com/crypto-gram/archives/2020/0315.html>
- Solvak, M., & Vassil, K. (2018). Could Internet voting halt declining electoral turnout? New evidence that e-voting is habit forming. *Policy & Internet*, 10(1), 4–21. <https://doi.org/10.1002/poi3.160>



REFERENCES

- Bula, R. (2025). Svitovyi dosvid e-vyboriv ta e-holosuvannia: Perspektyvy ta dosvid dlia Ukrainy [Global experience of e-elections and e-voting: Prospects and experience for Ukraine]. *Visnyk Lvivskoho universytetu. Seriiia filosofsko-politologichni studii*, 58, 242–250. <https://doi.org/10.30970/PPS.2025.58.30>
- Cabinet of Ministers of Ukraine. (n.d.). *Operatsiia "elektronizatsiia". Elektronne holosuvannia i pidrakhunok [Operation "electronization": Electronic voting and counting]*. <https://petition.kmu.gov.ua/petitions/2159>
- Council of Europe, Committee of Ministers. (2004, September 30). *Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*.
- Electronic voting in Estonia. (n.d.). In *Wikipedia*. https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia
- Encyclopaedia Britannica. (n.d.). *Voting machines*. <https://www.britannica.com/procon/voting-machines-debate>
- Hrynov, S. O., & Zakomorna, K. O. (2021). Elektronne holosuvannia: Perspektyvy vprovadzhennia v Ukraini ta zarubizhnyi dosvid [Electronic voting: Prospects for implementation in Ukraine and foreign experience]. *Yurydychni naukovyi elektronnyi zhurnal*, 4, 101–105. <https://doi.org/10.32782/2524-0374/2021-4/23>
- Gusarevych, N. (2022). Technological Solutions for Ensuring Electronic Voting in the Electoral Process: Foreign Experience. *Public Administration Aspects*, 10(1), 26–35. <https://doi.org/10.15421/152273>
- Khlaponin, Y., Vyshniakov, V., Prygara, M., & Poltorak, V. (2020). The new concept of guaranteeing confidence in the e-voting system. In *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)* (pp. 747–752). IEEE. <https://doi.org/10.1109/PICST51311.2020.9468012>
- Konstytutsiia Ukrainy [Constitution of Ukraine], Law of Ukraine No. 254k/96-VR. (1996). *Vidomosti Verkhovnoi Rady Ukrainy*, 30, Art. 141. <https://zakon.rada.gov.ua/laws/show/254k/96-вр#Text>
- Lisovskyi, Y. (2023, November 7). Internet-holosuvannia ta shkidlyve prohramne zabezpechennia: Pryklad Shveitsarii [Internet voting and malware: The example of Switzerland]. *Civil Network OPORA*. <https://www.oporaua.org/vybory/internet-golosuvannia-ta-shkidlyveprogramne-zabezpechennia-priklad-shveycariyi-24995>
- Mazur, O. (2020). Current tendencies of implementation of e-government in public administration: foreign experience. *Public Administration Aspects*, 7(12), 147–156. <https://doi.org/10.15421/151974>
- Pankratov, V. (2023). Elektronne holosuvannia yak element elektronnoi demokratii: Dosvid krain YeS [Electronic voting as an element of electronic democracy: The experience of EU countries]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriiia: Pravo*. <http://journal-app.uzhnu.edu.ua/article/view/294405/287190>
- Pro pravovyi rezhym voiennoho stanu [On the legal regime of martial law], Law of Ukraine No. 389-VIII. (2015). *Vidomosti Verkhovnoi Rady Ukrainy*, 28, Art. 250. <https://zakon.rada.gov.ua/laws/show/389-19#Text>
- Radio Svoboda. (2009, March 3). *U Nimechchyni zaboronyly elektronne holosuvannia na vyborakh [Electronic voting was banned in elections in Germany]*. <https://www.radiosvoboda.org/a/1503517.html>
- Romanenko, Ye. O. (2019). Elektronne holosuvannia – shliakh do vprovadzhennia elektronnykh mekhanizmiv demokratii v Ukraini [Electronic voting: A path to implementing electronic mechanisms of democracy in Ukraine]. *Publichne uriaduvannia*, 4(19), 259–271. [https://doi.org/10.32689/2617-2224-2019-4\(19\)-259-271](https://doi.org/10.32689/2617-2224-2019-4(19)-259-271)
- Schneier, B. (2004, November 1). *What's wrong with electronic voting machines?* Schneier on Security. https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html
- Schneier, B. (2020, March 15). *Voatz Internet voting app is insecure*. Schneier on Security. <https://www.schneier.com/crypto-gram/archives/2020/0315.html>
- Slovak, M., & Vassil, K. (2018). Could Internet voting halt declining electoral turnout? New evidence that e-voting is habit forming. *Policy & Internet*, 10(1), 4–21. <https://doi.org/10.1002/poi3.160>
- Topalova, S. (2020, April 30). Zapusk elektronnoho holosuvannia: Korysnyi dosvid Estonii [Launching electronic voting: Estonia's useful experience]. *LB.ua*. https://lb.ua/blog/svetlana_topalova/456467_zapusk_elektronnoho_golosuvannia.html
- Ukrainska Pravda. (2023, March 6). Vybori v Estonii: Vpershe v istorii ponad 50% vybortsiv holosuvaly onlain [Elections in Estonia: For the first time in history, more than 50% of voters voted online]. *Yevropeiska Pravda*. <https://www.eurointegration.com.ua/news/2023/03/6/7157420/>
- Vorona, P. V., Hoshovska, V. A., & Lopushynskyi, I. P. (2016). *Mistseva vlada v krainakh postradianskoho prostoru [Local government in post-Soviet countries]*. PP Shevchenko.
- Vyshniakov, V. M., Pryhara, M. P., & Voronin, O. V. (2014). Vidkryta systema taiemnoho holosuvannia [Open system of secret voting]. *Upravlinnia rozvytkom skladnykh system*, 20, 110–115.