УДК 324:004.738.5](474.2):234(477)
DOI https://doi.org/10.32782/2312-1815/2025-22-41

Олександр Фесенко
ORCID: 0009-0009-4715-9178

ЕСТОНСЬКА МОДЕЛЬ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ: АНАЛІЗ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ДЛЯ УКРАЇНИ

Стаття присвячена аналізу естонської моделі електронного голосування, яка поєднує високий рівень цифровізації з ефективними механізмами захисту та контролю. Розглянуто становлення системи i-Voting, її правові засади, технічні принципи роботи та роль інструментів електронної ідентифікації, зокрема ID-картки, Mobile-ID і цифрового підпису в Естонії. Продемонстровано, як комбінація криптографічного шифрування, перевірки факту врахування голосу та можливості повторного голосування забезпечує стабільність і надійність процесу волевиявлення. Наведено аналіз кіберінцидентів, які виявили вразливості у системі, та охарактеризовано, як вони сприяли посиленню безпекових стандартів і вдосконаленню процедур аудиту.

Окрему увагу приділено дискусії щодо впровадження мобільного голосування через смартфони, що потребує нових алгоритмів конфіденційності, сертифікації програмного забезпечення та ретельної оцінки ризиків. У контексті України розглянуто можливість адаптації естонського досвіду з опорою на наявні цифрові інструменти, насамперед застосунок «Дія», а також проаналізовано рівень підтримки цієї ініціативи, ризики витоку даних і виклики кіберзахисту в умовах воєнного стану.

У статті окреслено необхідні умови для запровадження електронного голосування в Україні: поетапну інтеграцію системи, поєднання електронного голосування з паперовими бюлетенями, підвищення кіберкультури громадян, розширення прав спостерігачів і створення прозорих процедур оскарження порушень під час голосування. Зазначено, що успішна імплементація можлива, але за умови застосування комплексного підходу та адаптації естонських практик до українського правового й безпекового середовища.

Ключові слова: *електронне голосування, кіберзахист, виборчий процес, застосунок «Дія», спостереження за виборами, Естонія, Україна, ЄС.*

Постановка проблеми. Забезпечення кіберзахисту систем електронного голосування є питанням стратегічного значення, особливо для таких країн, як Україна. Після завершення активних бойових дій перед державою постане нагальне завдання – забезпечити ефективну національну безпеку на всіх рівнях. Водночас в Україні зберігатиметься підвищена бойова готовність, що значно обмежить можливість участі значної частини громадян у виборчих процесах, зокрема через перебування на військовій службі та потенційні бойові ризики. Серед інших причин: втрата частиною виборців офіційних документів, що засвідчують їхню особу, внаслідок бойових дій; втрата можливості здійснювати волевиявлення безпосередньо на території виборчих дільниць з цих же причин; перебування значної кількості громадян за межами країни тощо. Одним із можливих рішень цих проблем є впровадження електронного голосування. Правильно спроєктовані системи електронного голосування можуть значно підвищити безпеку виборчого процесу, прискорити обробку результатів та зробити голосування доступнішим і зручнішим для громадян. Однак, якщо національна модель електронного голосування не буде ретельно продумана до найменших технічних і процедурних деталей, це може призвести до підриву довіри до виборчої системи загалом. У цьому контексті особливо важливим є звернення до міжнародного досвіду, зокрема європейського, що відповідає

євроінтеграційному курсу України. Однією з найрозвиненіших моделей електронного голосування є естонська система, яка стала взірцем для багатьох країн світу. Її досвід може стати основою для розробки надійної та ефективної національної системи електронного голосування в Україні.

Аналіз наукових досліджень свідчить, що питання переваг і недоліків упровадження електронного голосування вже тривалий час посідає важливе місце у зарубіжній науковій думці, серед яких виокремимо таких дослідників, як С. Гейберг, А. Парсовс та Ж. Віллемсон [24], які аналізують естонську модель електронного голосування 2013–2014 рр.; Х. Гарнетт і Т. Джеймс [23] розглядають електронні вибори як явище цифрового часу з акцентом на загрози та можливості, які технології становлять для цілісності виборчого процесу; Б. Вагнер [35] фокусує увагу на регуляторних викликах, пов'язаних з цифровим спостереженням за виборами та юридичним онлайн-контентом; Дж. Честер і К. Монтгомері [18] вказують на потенційні ризики, пов'язані із захистом особистих даних та маніпуляціями у виборчому процесі за допомогою інструментарію цифрової комунікації. Серед вітчизняних науковців відзначимо напрацювання таких авторів, як М. Афанасьєва, А. Береза, О. Бойко, Е. Войнова, О. Волкович, Р. Гаврік, М. Дворовий, А. Людва, О. Лізунова, О. Онуфрієв, М. Охендовський, О. Стогова, О. Токар-Остапенко, І. Щебетун, Є. Юрійчук та А. Комолов [36], які досліджують перспективи впровадження електронного голосування в Україні в контексті реалізації концепції розвитку електронної демократії, цифровізації та ін.

Методи дослідження. Автором застосовано системний підхід для аналізу функціонування електронного голосування в естонських реаліях, низку загальнонаукових методів, серед яких відзначимо порівняльний і соціологічний методи для оцінки результатів соціологічних досліджень з метою вивчення ставлення українців до електронного голосування та моделювання, пропонуючи відповідну вітчизняну модель. Статистичний метод дослідження дозволив системно проаналізувати дані щодо участі естонських виборців у електронному голосуванні й оцінити ефективність впровадженої моделі електронного волевиявлення.

Метою статті є аналіз основних складників естонської моделі електронного голосування, виокремлення її переваг і недоліків та визначення перспектив впровадження в Україні.

Результати й обговорення. Основні положення про електронне голосування викладені у низці національних нормативно-правових актів Естонії, зокрема законах Естонської Республіки «Про вибори Рійґікоґу» від 12.06.2002 р. [32], «Про вибори до місцевих рад» від 27.03.2002 р. [26], «Про вибори до Європейського парламенту» від 18.12.2002 р. [22] та «Про референдум» від 13.03.2002 р. [31], в яких детально регламентовано застосування електронного голосування у виборчих процесах на державному й муніципальних рівнях відповідно. У нормативно-правовому акті, що регулює організацію та проведення виборів до Рійґікоґу (естонського парламенту), виокремлено розділ, що присвячений підрахунку електронних голосів. Зокрема, Державна виборча служба має право анулювати ті голоси, які не містять реєстраційного номера кандидата, подані з порушеннями або не відповідають установленій формі. У контексті електронних виборів важливим є Закон «Про захист персональних даних» від 15.02.2007 р. [29], адже забезпечення конфіденційності та безпеки особистої інформації громадян є основою довіри до виборчої системи. Серед нормативно-правових актів, які регулюють цифрову спроможність проведення виборів, виокремлюємо закони «Про публічну інформацію» від 15.11.2000 р. [17] та «Про просторові дані» від 17.02.2011 р. [33].

Законодавчо урегульовано, що адмініструє систему електронного голосування, затверджує політику її інформаційної безпеки, електронні протоколи та технічні настанови Державна виборча служба. Вона також організовує усунення інцидентів, що перешкоджають голосуванню, визначає графік і обсяг тестування системи, затверджує його результати

та оприлюднює звіт. Крім того, Служба забезпечує проведення аудиту електронного голосування, під час якого перевіряється цілісність системи та відповідність нормативним актам. Натомість технічні вимоги та загальну організацію електронного голосування забезпечує Національна виборча комісія [4, с. 61].

Ключовим елементом участі в електронному голосуванні для кожного естонця є національне електронне посвідчення особи (ID-kaart). Воно слугує базовим засобом ідентифікації в електронному середовищі та використовується для створення електронного підпису [21]. Саме ж голосування здійснюється через офіційний клієнтський застосунок i-Voting (IVCA), через який виборець може завантажити список кандидатів та відправити свій голос за одного з них на сервер. Програмне забезпечення для голосування доступне для Windows, macOS та Linux, тоді як смартфон може використовуватися лише для перевірки поданого голосу за допомогою спеціального застосунку та QR-коду [24, p. 20].

Функція перевірки голосу є важливою, адже в Естонії дозволено голосувати онлайн необмежену кількість разів, і враховується виключно останній голос, поданий до завершення періоду електронного волевиявлення [20]. На парламентських виборах 2023 р. 10,787 електронних голосів було замінено, на муніципальних виборах 2024 р. – 23,598 [34]. Подібний механізм перевірки вибору через QR-код використовують також у Бельгії, де це можна зробити безпосередньо на виборчій дільниці [30].

Електронне голосування організовує Державна виборча служба у співпраці з Управлінням інформаційних систем. Перед його початком Служба готує відповідну систему та розміщує застосунок виборця на вебсайті valimised.ee. Процес голосування розпочинається у понеділок виборчого тижня о 9:00 та завершується у суботу о 20:00. Для участі у голосуванні виборець має завантажити застосунок на комп'ютер. Застосунок автоматично перевіряє право виборця голосувати та відображає коректний список кандидатів. Після здійснення вибору застосунок шифрує голос. Виборець підтверджує його своїм цифровим підписом, після чого застосунок передає зашифрований бюлетень на сервер збору голосів. Одночасно незалежна служба реєстрації додає до кожного голосу позначку часу, що дозволяє пізніше перевірити, чи всі голоси були передані правильно. Інтернет-голоси шифруються за допомогою сучасних криптографічних алгоритмів. Точну специфікацію алгоритму щоразу перед виборами визначає Державна виборча служба. Голос шифрується за допомогою двох ключів: застосунок виборця використовує публічний ключ шифрування, а ключ для розшифрування бюлетенів зберігається виключно у членів Національної виборчої комісії.

В Естонії електронне голосування вважається таким, що відбулося без технічних помилок і загроз безпеці, якщо відповідає таким факторам:

1) Відповідність засобів електронної ідентифікації. Голос виборця має бути зашифрований і підписаний тим самим інструментом, яким він пройшов ідентифікацію.

2) Стабільність IP-адреси та операційної системи під час голосування. Якщо змінюється IP-адреса або операційна система виборця під час голосування, це може свідчити про спробу впливу на процес голосування сторонніми особами.

3) Унікальність криптограми голосу. Голос виборця шифрується за допомогою унікальної криптограми (абревіатури або знаків). Повторення зашифрованих голосів може вказувати на помилку або на спробу втручання через шкідливе програмне забезпечення, або атаку, спрямовану на копіювання бюлетенів.

4) Перевіряються тільки ідентифікатори, видані системою. Якщо запит на перевірку голосу містить ідентифікатор, який система не видавала, це також може бути ознакою атаки на систему або технічної помилки в i-Voting [24, p. 23].

«Слабкою ланкою» в електронному голосуванні традиційно залишається пристрій виборця, насамперед персональний комп'ютер. У 2011 р. виборець Пааво Піхельгас створив

троян-вірус, який дозволяв маніпулювати вибором та змінювати подані голоси [27]. Інший громадянин Естонії, Мярт Пидер, у 2015 р. зумів вкинути до системи недійсний електронний бюлетень. У 2023 р. йому вдалося створити інструмент, який дозволяв завантажувати на комп'ютер зашифровані голоси з подальшою можливістю їх дешифрування. Попри це, подібні інциденти не стали руйнівними для естонської моделі, навпаки, вони дали змогу виявити недоліки та підвищити рівень захисту. Серед пропозицій – впровадження системи наскрізної верифікації, тобто послідовний процес підтвердження достовірності даних, документів або особи на всіх етапах взаємодії між виборцем та додатком для голосування [28].

Отже, естонці можуть голосувати онлайн виключно за допомогою персональних комп'ютерів. Для того щоб вони могли голосувати через смартфони, необхідно, на думку міністра економіки та інформаційних технологій Естонії Тійта Рійсала, впровадити систему моніторингу даних. Водночас є труднощі з розміщенням додатків для голосування на популярних платформах, таких як Google та Apple [7].

Можливість запровадження мобільного онлайн-голосування обговорювалася під час розробки програми mRiik – «держави в смартфоні», яка створювалася спільно з українськими розробниками на основі української «Дії». Однак ініціатива дещо пригальмувала, згідно з офіційною версією, через відмінність естонських та українських реєстрів [6]. Через високі вимоги до конфіденційності деякі етапи обробки голосів повинні виконуватися безпосередньо на пристрої користувача, а не на сервері, тому для мобільного голосування був розроблений спеціальний застосунок, у тестуванні якого в 2025 р. взяли участь 2,430 естонців із 29 країн світу [25].

Отож, в Естонії цілком серйозно обговорюється питання впровадження голосування через смартфони. Електронне голосування там зокрема здійснюється за допомогою мобільного телефону зі сертифікованою SIM-карткою (mobile-ID SIM), підключеного до комп'ютера. Виборець має заздалегідь отримати PIN-коди та мати цифровий підпис. Уперше цей механізм застосували у 2011 р. на виборах Рійґікоґу. Для голосування телефон під'єднується до комп'ютера, виборець заходить на відповідний сайт і запускає застосунок: PIN 1 використовується для ідентифікації, а PIN 2 – для підтвердження вибору [3, с. 115]. Водночас, на нашу думку, реалізація такого способу голосування в Україні на сучасному етапі була б доволі складною.

З огляду на успішний досвід впровадження мобільних додатків на кшталт «Дії», питання електронного голосування вже стоїть на порядку денному в Україні. Відповідний запит у суспільства вже давно фігурує у вітчизняному інтернет-просторі – на сайті Президента України зареєстрована петиція щодо проведення виборів у додатку «Дія» [15]. Основний аргумент на боці впровадження цієї інновації – «Дії» доступні офіційні документи громадян та прив'язка до банківської мережі, що значно спростить виборчі процеси, зокрема на етапах реєстрації виборчого корпусу [5]. Частково ці ідеї знайшли відображення у «Профілі виборця», який доступний у додатку, що дозволяє користувачу «Дії» перевірити наявність у списку виборців, дізнатися свою виборчу дільницю та отримати всю необхідну інформацію щодо виборів у разі втрати офіційного запрошення [16]. Однак петиції щодо впровадження електронного голосування не змогли набрати достатньої кількості підписів, що свідчить про недостатній рівень довіри суспільства до цієї ідеї. Це підтверджують результати соціологічного опитування: станом на 2024 р. менше половини виборців (42–43%) негативно ставляться до інтернет-виборів; близько третини респондентів (31%) вважають, що у разі запровадження електронного голосування воно має здійснюватися через «Дію»; ще 15% переконані, що для цього необхідно створити окремий спеціалізований сервіс. Водночас 37,5% наголошують, що виборче голосування взагалі не повинно проводитися в електронному форматі [3, с. 61]. На думку Міністра цифрової трансформації України Михайла

Федорова, впровадження електронного голосування обов'язково повинне супроводжуватися суспільною підтримкою, відповідним рішенням ЦВК, змінами до виборчого законодавства, що, зважаючи зокрема на результати соціологічних опитувань, нині не спостерігається в українських реаліях [8]. А Голова Верховної Ради Руслан Стефанчук переконаний, що проведення електронних виборів є політизованим питанням, на основі якого можуть виникнути різноманітні спекуляції та закиди з боку опозиційних до чинної влади політичних діячів та громадськості [9].

Основою правового регулювання цифровізації виборчих процесів в Україні нині є відповідні нормативно-правові акти, які після 2020 р. зазнали низки доповнень і коригувань. До них належать Виборчий кодекс України від 19.12.2019 р. № 396-IX [2], закони України: «Про Центральну виборчу комісію» від 30.06.2004 р. № 1932-IV [14], «Про політичні партії в Україні» від 5.04.2001 р. № 2365-III [13], «Про електронні документи та електронний документообіг» від 22.05.2003 р. № 851-IV [11], «Про електронну ідентифікацію та електронні довірчі послуги» від 5.10.2017 р. № 2155-VIII [12], «Про Державний реєстр виборців» від 22.02.2007 р. № 698-V [10] та ін. Проте процедура електронного голосування в них детально не регламентована.

Натомість досвід Естонії демонструє, що електронні вибори є дієвим засобом, який не одразу, але з певним проміжком часу може стати інструментом, що заслуговує на суспільну довіру та легітимує вибрані у такий спосіб органи державної влади та місцевого самоврядування. Цю тезу яскраво підтверджує динаміка результатів голосування на виборах до Рійгікоґу та місцевих виборах, де кількість учасників електронного голосування щоразу збільшувалася (див. Табл. 1).

Таблиця 1

Частка естонських виборців серед загального виборчого корпусу, які взяли участь в електронному голосуванні (%)

Парламентські вибори (%)		**Муніципальні вибори**	
2023 р.	32,5	2021 р.	25,7
2019 р.	27,9	2017 р.	16,9
2015 р.	19,6	2013 р.	12,3
2011 р.	12,3	2009 р.	9,5
2007 р.	3,4	2005 р.	0,9

Джерело: складено автором на основі [34]

Незважаючи на успішний досвід цифровізації окремих послуг в Україні, формування довіри до електронного голосування, на нашу думку, все ж буде тривалим поступовим процесом. Знадобиться певний час, аби значна кількість виборців підтримала таку форму голосування. На наш погляд, вітчизняна модель електронного голосування та підрахунку голосів повинна бути впроваджена таким чином, щоби не порушувати виборчі стандарти та має мати такі складники:

1. *Створення спеціального додатка, через який проводилися б вибори, або модернізація порталу «Дія» до рівня, здатного забезпечити демократичне волевиявлення.* Хоча, на переконання М. Федорова, система буде готова до проведення виборів лише після оцінки результатів упровадження електронного голосування за петиції. На основі цих результатів ухвалюватиметься рішення щодо запуску електронного голосування [1]. В Україні вже є успішні кейси створення якісних додатків, зокрема вже згадана «Дія», а також таких, які мають прямий зв'язок із військовою службою («Резерв+», «Армія+»), що значно спрощують отримання адміністративних послуг без фізичної присутності в офіційних інституціях.

Інше питання – забезпечення надійного кіберзахисту для зазначених вище додатків. Особливо це стосується додатків, які пов'язані з проходженням військової служби. Наприклад, якщо український військовослужбовець потрапить у полон, ворог зможе без особливих труднощів отримати доступ до додатків, адже, окрім підтвердження через Face ID (що у «Резерв+» є опціональною функцією) та чотиризначного пароля, інших варіантів захисту немає. Запровадження згаданої вище наскрізної верифікації може частково зменшити ризики маніпуляцій голосами, зокрема у випадках, коли хтось інший може скористатися телефоном виборця та проголосувати замість нього. Водночас такий підхід потенційно ускладнить процес електронного голосування, що може негативно позначитися на його зручності та, відповідно, на рівні підтримки серед громадян. Тому на початковому етапі впровадження електронного голосування в Україні вважаємо доцільним використання його паралельно з традиційним способом голосування – паперовими бюлетенями. Для ідентифікації виборця можна використовувати BankID, «Дію» та електронний підпис як засіб подання голосу, але за умови, що будуть дотримані всі необхідні умови для належного захисту даних.

2. *Надійне шифрування поданого голосу для забезпечення таємності голосування через BankID або інші способи авторизації.* На парламентських виборах пропонується, щоб виборці завантажували список партій або кандидатів, якщо це мажоритарний округ. За схожим принципом працювали б вибори на місцевому рівні. Для виборця, залежно від його місця проживання, формується відповідний список кандидатів та партій. Відповідно, в базі повинні бути внесені всі дані про виборців та округ, за яким вони закріплені. У разі зміни місця проживання виборець повинен буде подати відповідні відомості у відповідні структури, щоб зміни були враховані.

3. *Можливість перевірки факту врахування або неврахування голосу виборця.* Згідно з естонським законодавством, підрахунок голосів, поданих через Інтернет, відбувається відкрито членами виборчої комісії на виборчій дільниці, що забезпечує принцип таємності голосування. Однак постає питання: як виборцю перевірити поданий ним голос, себто за якого кандидата він проголосував, і чи був врахований його голос взагалі. Естонський досвід цілком слушно дозволяє перевірити лише *факт врахування або неврахування голосу*, подібно до фізичного вкидання бюлетеня у скриньку на виборчій дільниці. Якщо бюлетень вкинуто, то перевірити, за кого був відданий голос, неможливо. Переконатися в правильності свого вибору можна на етапі голосування в кабінці до того, як бюлетень потрапить до скриньки. Схожий принцип можна реалізувати й у смартфоні, коли виборець може поставити електронну позначку навпроти імені кандидата чи назви партії та переконатися у правильності свого вибору до того, як голос буде відправлений у віртуальну скриньку.

4. *Врахування супутніх ризиків і проблем* (відсутність прозорості; недовіра до процесу; складнощі інноваційного способу для виборців та необхідність проведення для них широкомасштабної освіти щодо кіберзахисту; труднощі з аудитом результатів; забезпечення таємниці голосування; безпека процесу голосування та підрахунку голосів; вартість впровадження та обслуговування технології; забезпечення контролю технологій; наявність персоналу зі спеціалізованими навичками в галузі ІТ тощо). Відповідальна інституція, наприклад ЦВК або Міністерство цифрової трансформації, повинна ретельно фіксувати всі проблеми, потенційні ризики, а в період без виборів – тестувати систему після кожного оновлення та модернізації. У випадку технічних збоїв або виявлення стороннього впливу на виборчий процес є потенційна можливість переголосування або на виборчій дільниці, із публічним оголошенням про виявлені проблеми, за допомогою паперового бюлетеня, або повторно через Інтернет, якщо ці проблеми були усунені. Цілком можливо, що відповідна процедура була б передбачена в українській моделі електронного голосування.

У більшості моментів можемо спостерігати деякі елементи естонської моделі, які цілком могли б знайти місце на вітчизняній площині у зв'язку з уже наявними інструментами. Основний ризик полягає в потенційному витоку даних про виборців та їхній вибір, що не раз траплялося з «Дією», коли інформація про користувачів опинялася в публічному доступі, а тому для мінімізації цього ризику питання кібербезпеки виходить на перший план, яка передбачає не тільки технологічні рішення, а й підвищення кіберграмотності виборців зокрема (за прикладом Бельгії). Це включає рекомендації щодо використання двофакторної автентифікації, встановлення лише ліцензійного програмного забезпечення – особливо антивірусного – та загальне розуміння основних принципів безпечної цифрової поведінки [19, p. 5]. Така практика є доречною і для України, адже рівень кіберкультури громадян прямо впливає на безпеку всього процесу електронного голосування та підрахунку голосів.

Однак, попри інноваційність та успіх естонської моделі електронного голосування, а також високий рівень кіберзахисту, постають важливі питання щодо забезпечення якісного спостереження за виборчим процесом для забезпечення громадської довіри та загальної чесності виборів як демократичного інституту, що можливо лише за умов повної прозорості та підзвітності. Експерти наголошують на кількох ключових рекомендаціях.

По-перше, спостерігачі повинні мати *реальне право оскаржувати результати голосування*. В Естонії досі немає чіткого правового визначення випадків, коли результати електронного волевиявлення можуть бути визнані частково або повністю недійсними. До того ж відповідні процедури фактично приховані від спостерігачів, що суперечить принципу відкритості виборів.

По-друге, спостерігачі повинні отримати *доступ до всіх етапів електронного голосування*: формування списків виборців, підготовки обладнання, встановлення та запуску програмного забезпечення, а також до моменту надання доступу виборцям. Нині в Естонії цей доступ забезпечено лише частково, що не дозволяє назвати модель повністю спостережуваною.

По-третє, *спостереження має охоплювати не лише перевірку результатів голосування, а й усі процеси, пов'язані з організацією електронних виборів*. Незалежні спостерігачі повинні мати можливість перевірити, чи програмне забезпечення пройшло сертифікацію, належні процедури аудиту та чи належним чином задокументована історія його використання.

По-четверте, *строки оскарження мають починати відлік не з моменту виникнення події, а з моменту, коли вона стала відомою*. Наприклад, якщо невідповідність у кількості голосів, підрахованих 5 березня, стала публічною лише 8 березня, то вимога оскаржити її того ж дня фактично унеможливлює реальний механізм захисту прав виборців.

По-п'яте, *повний пакет інформації щодо організації, підготовки та проведення електронних виборів має надаватися спостерігачам завчасно*. Це дозволить їм ознайомитися з роботою системи, програмними кодами, документацією та визначити потенційні ризики ще до старту виборів [20]. Відповідно, впроваджуючи електронне голосування в Україні, доцільно врахувати зазначені вище фактори, оскільки вони сприятимуть забезпеченню легітимності виборчого процесу, особливо з огляду на новизну такої практики для нашої держави.

Висновки. Естонія успішно застосовує електронне голосування та підрахунок голосів у виборчих процесах, однак там і надалі фіксують певні проблеми, пов'язані з кіберзахистом та забезпеченням належного контролю за голосуванням, зокрема через втручання окремих громадян у вибори та відсутність належних контролюючих можливостей у спостерігачів. Україна теоретично могла б упровадити подібну модель, проте естонський досвід і недостатня готовність українського суспільства свідчать про необхідність подальшого вдосконалення

цієї практики перед її впровадженням, а також про забезпечення надійного захисту електронного волевиявлення у застосунку та організацію якісної освіти українських виборців з питань кібербезпеки. Перспектива подальших досліджень полягає в пошуку найоптимальнішої моделі електронного голосування, яка буде прийнятною для сучасних українських реалій, забезпечуватиме дотримання принципів демократичного голосування, ефективне спостереження та гарантуватиме довіру з боку суспільства та міжнародної спільноти.

Література:

1. Вибори президента в «Дії». Федоров назвав умови, за яких це стане можливо. URL: https://dou.ua/lenta/news/fedorov-about-elections-in-diya/ (дата звернення: 06.12.2025).

2. Виборчий кодекс України : Закон України від 19.12.2019 р. № 396-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/396-20#Text (дата звернення: 12.12.2025).

3. Війна і майбутні вибори в Україні: виклики та перспективи. Національна безпека і оборона. 2024. № 1–2 (195–196). 117 с. URL: https://razumkov.org.ua/images/2024/10/28/NSD195-196_2023_ukr.pdf (дата звернення: 06.12.2025).

4. Гаврік Р. О. Естонський досвід здійснення електронного голосування: перспективи запровадження в Україні. Економіка. Фінанси. Право. 2023. № 6. С. 60–63. DOI: https://doi.org/10.37634/efp.2023.6.13.

5. Голосування через додаток ДІЯ. Офіційне інтернет-представництво Президента України. URL: https://petition.president.gov.ua/petition/125898 (дата звернення: 06.12.2025).

6. Естонія не робитиме застосунок держпослуг на базі «Дії», тендер отримала місцева IT-компанія. URL: https://dou.ua/lenta/news/development-mriik-diia-estonia/ (дата звернення: 06.12.2025).

7. Естонці голосуватимуть на виборах у смартфоні. А ви б наважилися? URL: https://dou.ua/forums/topic/48901/ (дата звернення: 06.12.2025).

8. Зінченко М. Питання проведення виборів у «Дії» не стоїть – Федоров. 2025. URL: https://detector.media/infospace/article/239119/2025-03-17-pytannya-provedennya-vyboriv-u-dii-ne-stoit-fedorov/ (дата звернення: 06.12.2025).

9. Мельник Р. Стефанчук про можливі вибори через «Дію»: Це нереалістично. 2025. URL: https://hromadske.ua/polityka/243023-stefanchuk-pro-mozlyvi-vybory-cherez-diiu-tse-nerealistychno (дата звернення: 06.12.2025).

10. Про Державний реєстр виборців : Закон України від 22.02.2007 р. № 698-V. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/698-16#Text (дата звернення: 12.12.2025).

11. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 12.12.2025).

12. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5.10.2017 р. № 2155-VIII. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 12.12.2025).

13. Про політичні партії в Україні : Закон України від 5.04.2001 р. № 2365-III. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2365-14#Text (дата звернення: 12.12.2025).

14. Про Центральну виборчу комісію : Закон України від 30.06.2004 р. № 1932-IV. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1932-15#Text (дата звернення: 12.12.2025).

15. Проведення виборів за допомогою порталу Дія, створення найкращих умов у зв'язку зі зменшенням кількості осіб, які були залучені до виборчого процесу, для більшості виборців, зменшення затрат на проведення виборів місцевих, президентських та до Верховної Ради. Офіційне інтернет-представництво Президента України. URL: https://petition.president.gov.ua/petition/126080 (дата звернення: 06.12.2025).

16. Профіль виборця в Дії. Дія. URL: https://diia.gov.ua/news/profil-viborcya-v-diyi (дата звернення: 06.12.2025).

17. Avaliku teabe seadus: Vastu võetud 15.11.2000. Riigi Teataja. URL: https://www.riigiteataja.ee/akt/106012016007#para43b9lg1p3 (дата звернення: 10.12.2025).

18. Chester J., Montgomery K. The role of digital marketing in political campaigns. *Internet Policy Review*. 2017. № 6 (4). P. 1–20.

19. De Bruycker M., Bostyn F., Dutron S. Safe Surfing during the Belgian General Election Campaign: Recommendations for a cybersecure electoral campaign. 2024. 15 p. URL: https://vsse.be/sites/default/files/2025-06/elections-2024-uk-alt-web-v3_0.pdf (дата звернення: 03.12.2025).

20. Demand for observable e-Voting. Joint statement of election observers on 31st of March 2023. URL: https://ausadvalimised.ee/en/docs/yhisavaldus2023/ (дата звернення: 03.12.2025).

21. Digital ID. Politsei- ja Piirivalveamet. URL: https://www.politsei.ee/en/instructions/digital-id (дата звернення: 01.12.2025).

22. European Parliament Election Act: Passed 18.12.2002. *Riigi Teataja.* URL: https://www.riigiteataja.ee/en/eli/ee/529012014001/consolide/current (дата звернення: 10.12.2025).

23. Garnett H., James T. Cyber Elections in the Digital Age: Threats and Opportunities of technology for electoral integrity. *Election Law Journal*. 2020. № 19 (2). P. 111–126.

24. Heiberg S., Parsovs A., Willemson J. Log Analysis of Estonian Internet Voting 2013–2014. *Cryptology ePrint Archive*. 2015. Vol. 1211. P. 19–34. DOI: https://doi.org/10.1007/978-3-319-22270-7_2 (дата звернення: 01.12.2025).

25. Marius Comper. More than 2.400 Estonians worldwide took part this week in the country's first public test of a new mobile online voting app. May 23, 2025. URL: https://www.facebook.com/marius.comper/posts/-more-than-2400-estonians-worldwide-took-part-this-week-in-the-countrys-first-pu/10162728835749621/ (дата звернення: 09.12.2025).

26. Municipal Council Election Act. Passed 27.03.2002. *Riigi Teataja*. URL: https://www.riigiteataja.ee/en/eli/ee/514112016001/consolide/current (дата звернення: 01.12.2025).

27. OSCE findings on Estonian e-Voting. 2011. URL: https://edri.org/our-work/edrigramnumber9-11e-voting-osce-estonia/ (дата звернення: 07.12.2025).

28. Perils of e-Voting in Estonia. Märt Põder. 2023. URL: https://infoaed.ee/interventions_2023.pdf (дата звернення: 03.12.2025).

29. Personal Data Protection Act: Passed 15.02.2007. *Riigi Teataja*. URL: https://www.riigiteataja.ee/en/eli/507032016001/consolide (дата звернення: 10.12.2025).

30. Puis-je vérifier mon bulletin de vote? (vote électronique). Service public fédéral Intérieur. *Elections*. URL: https://elections.fgov.be/node/111460 (дата звернення: 01.12.2025).

31. Referendum Act: Passed 13.03.2002. *Riigi Teataja.* URL: https://www.riigiteataja.ee/en/eli/514112013007/consolide/current (дата звернення: 10.12.2025).

32. Riigikogu Election Act: Passed 12.06.2002. *Riigi Teataja.* URL: https://www.riigiteataja.ee/en/eli/ee/513012020001/consolide/current.

33. Ruumiandmete seadus: Vastu võetud 17.02.2011. *Riigi Teataja*. URL: https://www.riigiteataja.ee/akt/110032017002#para58lg1 (дата звернення: 10.12.2025).

34. Statistics about Internet voting in Estonia. *Valimised*. URL: https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia (date of access: 9.12.2025).

35. Wagner B. Digital Election Observation: Regulatory Challenges around Legal Online Content. *The Political Quarterly*. 2020. № 91(4). P. 739–744.

36. Yurichuk Ye., Komolov A. Civil society control over the use of digital technologies in the electoral process in the context of European integration. *Mediaforum*. 2023. № 12. P. 170–181.

References:

1. Vybory prezydenta v «Dii» [Presidential elections in "Diia". Fedorov named the conditions under which this will be possible]. (n.d.). *dou.ua.* Retrieved from: https://dou.ua/lenta/news/fedorov-about-elections-in-diya/ [in Ukrainian].

2. Vyborchyi kodeks Ukrainy [Electoral Code of Ukraine]. (2019, December 19). Zakon Ukrainy No. 396-IX. *zakon.rada.gov.ua.* Retrieved from: https://zakon.rada.gov.ua/laws/show/396-20#Text [in Ukrainian].

3. Natsionalna bezpeka i oborona. (2024). Viina i maibutni vybory v Ukraini: vyklyky ta perspektyvy [War and upcoming elections in Ukraine: challenges and prospects]. *Natsionalna bezpeka i oborona – National*

Security and Defence, 1–2(195–196), 117. Retrieved from: https://razumkov.org.ua/images/2024/10/28/NSD195-196_2023_ukr.pdf [in Ukrainian].

4. Havrik, R.O. (2023). Estonskyi dosvid zdiisnennia elektronnoho holosuvannia: perspektyvy zaprovadzhennia v Ukraini [Estonian experience of electronic voting: prospects of implementation in Ukraine]. *Ekonomika. Finansy. Pravo – Economics. Finance. Law*, (6), 60–63 [in Ukrainian].

5. Ofitsiine internet-predstavnytstvo Prezydenta Ukrainy. (n.d.). Holosuvannia cherez dodatok DIYa [Voting via the Diia app]. *petition.president.gov.ua.* Retrieved from: https://petition.president.gov.ua/petition/125898 [in Ukrainian].

6. Estoniia ne robytyme zastosunok derzhposluh na bazi «Dii», tender otrymala mistseva IT-kompaniia [Estonia will not make a public services application based on "Diya", a local IT company won the tender]. (n.d.). *dou.ua.* Retrieved from: https://dou.ua/lenta/news/development-mriik-diia-estonia/ [in Ukrainian].

7. Estontsi holosuvatymut na vyborakh u smartfoni. A vy b navazhylysia? [Estonians will vote in the elections on their smartphones. Would you dare?]. (n.d.). *dou.ua.* Retrieved from: https://dou.ua/forums/topic/48901/ [in Ukrainian].

8. Zinchenko, M. (2025). Pytannia provedennia vyboriv u «Dii» ne stoit, – Fedorov [The issue of holding elections is not on the agenda in "Diya", – Fedorov]. *detector.media.* Retrieved from: https://detector.media/infospace/article/239119/2025-03-17-pytannya-provedennya-vyboriv-u-dii-ne-stoit-fedorov/ [in Ukrainian].

9. Melnyk, R. (2025). Stefanchuk pro mozhlyvi vybory cherez «Diiu»: Tse nerealistychno [Stefanchuk on possible elections through "Diya": This is unrealistic]. *hromadske.ua.* Retrieved from: https://hromadske.ua/polityka/243023-stefanchuk-pro-mozlyvi-vybory-cherez-diiu-tse-nerealistychno [in Ukrainian].

10. Pro Derzhavnyi reiestr vybortsiv [On the State Register of Voters]. (2007, February 22). Zakon Ukrainy No. 698-V. *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/698-16#Text [in Ukrainian].

11. Pro elektronni dokumenty ta elektronnyi dokumentoobih [On Electronic Documents and Electronic Documents Flow]. (2003, May 22). Zakon Ukrainy No. 851-IV. *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/851-15#Text [in Ukrainian].

12. Pro elektronny identyfikatsiiu ta elektronni dovirchi posluhy [On Electronic Identification and Trust Services]. (2017, October 5). Zakon Ukrainy No. 2155-VIII. *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/2155-19#Text [in Ukrainian].

13. Pro politychni partii v Ukraini [On Political Parties in Ukraine]. (2001, April 5). Zakon Ukrainy No. 2365-III. *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/2365-14#Text [in Ukrainian].

14. Pro Tsentralnu vyborchu komisiiu [On the Central Election Commission]. (2004, June 30). Zakon Ukrainy No. 1932-IV. *zakon.rada.gov.ua*. Retrieved from: https://zakon.rada.gov.ua/laws/show/1932-15#Text [in Ukrainian].

15. Ofitsiine internet-predstavnytstvo Prezydenta Ukrainy. (n.d.). Provedennia vyboriv za dopomohoiu portalu Diia, stvorennia naikrashchikh umov u zviazku zi zmensheniam kilkosti osib yaki buly zalucheni do vyborchoho protsessu, dlia bilshosti vybortsiv, zmenshyty zatraty na provedennia vyboriv mistsevykh, prezydentskykh, ta u Verkhovnu Radu [Conducting elections using the Diya portal, creating the best conditions for the majority of voters due to the reduction in the number of people involved in the electoral process, reducing the costs of conducting local, presidential, and Verkhovna Rada elections]. *Petition.president.gov.ua.* Retrieved from: https://petition.president.gov.ua/petition/126080 [in Ukrainian].

16. Diia. (n.d.). Profil vybortsia v Dii [Voter profile in Diya]. *diia.gov.ua.* Retrieved from: https://diia.gov.ua/news/profil-viborcya-v-diyi [in Ukrainian].

17. Riigi Teataja. (2000, November 15). Avaliku teabe seadus [Public Information Act]. *Riigiteataja.ee.* Retrieved from: https://www.riigiteataja.ee/akt/106012016007#para43b9lg1p3 [in Estonian].

18. Chester, J., & Montgomery, K. (2017). The role of digital marketing in political campaigns. *Internet Policy Review*, 6(4), 1–20.

19. De Bruycker, M., Bostyn, F., & Dutron, S. (2024). Safe surfing during the Belgian general election campaign: Recommendations for a cybersecure electoral campaign. *vsse.be.* (15 pp.). Retrieved from: https://vsse.be/sites/default/files/2025-06/elections-2024-uk-alt-web-v3_0.pdf.

20. Joint statement of election observers on 31st of March 2023. (2023). Demand for observable e-Voting. *ausadvalimised.ee.* Retrieved from: https://ausadvalimised.ee/en/docs/yhisavaldus2023/.

21. Politsei- ja Piirivalveamet. (n.d.). Digital ID. *politsei.ee.* Retrieved from: https://www.politsei.ee/en/instructions/digital-id.

22. Riigi Teataja. (2002, December 18). European Parliament Election Act. *riigiteataja.ee.* Retrieved from: https://www.riigiteataja.ee/en/eli/ee/529012014001/consolide/current.

23. Garnett, H., & James, T. (2020). Cyber elections in the digital age: Threats and opportunities of technology for electoral integrity. *Election Law Journal*, 19(2), 111–126.

24. Heiberg, S., Parsovs, A., & Willemson, J. (2015). Log analysis of Estonian internet voting 2013–2014. *Cryptology ePrint Archive*, 1211, 19–34.

25. Comper, M. (2025, May 23). More than 2.400 Estonians worldwide took part this week in the country's first public test of a new mobile online voting app. *facebook.com.* Retrieved from: https://www.facebook.com/marius.comper/posts/-more-than-2400-estonians-worldwide-took-part-this-week-in-the-countrys-first-pu/10162728835749621/.

26. Riigi Teataja. (2002, March 27). Municipal Council Election Act. *riigiteataja.ee.* Retrieved from: https://www.riigiteataja.ee/en/eli/ee/514112016001/consolide/current.

27. OSCE findings on Estonian e-Voting. (2011). *Edri.org.* Retrieved from: https://edri.org/our-work/edrigramnumber9-11e-voting-osce-estonia/.

28. Põder, M. (2023). Perils of e-Voting in Estonia. *Infoaed.ee.* Retrieved from: https://infoaed.ee/interventions_2023.pdf.

29. Riigi Teataja. (2007, February 15). Personal Data Protection Act. *Riigiteataja.ee.* Retrieved from: https://www.riigiteataja.ee/en/eli/507032016001/consolide.

30. Service public fédéral Intérieur. (n.d.). Puis-je vérifier mon bulletin de vote? (vote électronique) [Can I check my ballot? (electronic voting)]. *elections.fgov.be.* Retrieved from: https://elections.fgov.be/node/111460 [in French].

31. Riigi Teataja. (2002, March 13). Referendum Act. *riigiteataja.ee.* Retrieved from: https://www.riigiteataja.ee/en/eli/514112013007/consolide/current.

32. Riigi Teataja. (2002, June 12). Riigikogu Election Act. *riigiteataja.ee.* Retrieved from: https://www.riigiteataja.ee/en/eli/ee/513012020001/consolide/current.

33. Riigi Teataja. (2011, February 17). Ruumiandmete seadus [Spatial Data Act]. *riigiteataja.ee.* Retrieved from: https://www.riigiteataja.ee/akt/110032017002#para58lg1 [in Estonian].

34. Valimised. (n.d.). Statistics about internet voting in Estonia. *valimised.ee.* Retrieved from: https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia.

35. Wagner, B. (2020). Digital election observation: Regulatory challenges around legal online content. *The Political Quarterly*, 91(4), 739–744.

36. Yurichuk, Ye., & Komolov, A. (2023). Civil society control over the use of digital technologies in the electoral process in the context of European integration. *Mediaforum*, 12, 170–181.

Oleksandr Fesenko. The Estonian Model of Electronic Voting: Analysis and Prospects for Implementation in Ukraine

The article examines the Estonian model of electronic voting, which combines a high level of digitalization with effective security and control mechanisms. It provides a detailed analysis of the development of the i-Voting system, its legal foundations, technical operating principles, and the role of electronic identification tools, including the ID-card, Mobile-ID, and digital signature. The study demonstrates how the combination of cryptographic encryption, verification of vote inclusion, and the possibility of re-voting ensures the stability and reliability of the electoral process. It also presents an analysis of cyber incidents that revealed system vulnerabilities and describes how these incidents contributed to strengthening security standards and improving audit procedures.

Special attention is given to the discussion about implementing mobile voting via smartphones, which requires new confidentiality algorithms, software certification, and a careful assessment of potential risks. In the context of Ukraine, the article considers the possibility of adapting the Estonian experience by relying on

existing digital tools, particularly the Diia application, and analyzes the level of support for this initiative, risks of data leaks, and cybersecurity challenges in wartime conditions.

The article outlines the essential prerequisites for introducing electronic voting in Ukraine: gradual system integration, maintaining parallel paper-ballot voting, improving citizens cyber literacy, expanding observers rights, and establishing transparent procedures for appeals. It emphasizes that successful implementation is possible only under a comprehensive approach and proper adaptation of Estonian practices to the Ukrainian legal and security environment.

Key words: *electronic voting, cybersecurity, electoral process, Diia application, election monitoring, Estonia, Ukraine, EU.*

Відомості про автора:

Фесенко Олександр – аспірант кафедри політології та державного управління, Чернівецький національний університет імені Юрія Федьковича.

Дата першого надходження статті до видання: 12.12.2025
Дата прийняття статті до друку після рецензування: 31.12.2025
Дата публікації (оприлюднення) статті: 28.01.2026