

ПРАВОВІ РИЗИКИ ВПРОВАДЖЕННЯ BLOCKCHAIN У СФЕРУ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ: ДОСВІД ТА УРОКИ МІЖНАРОДНОЇ ПРАКТИКИ

Тарас Романович ЗАЙКА,

*аспірант відділу організації
освітньої-наукової підготовки
Харківського національного
університету внутрішніх справ*

Інноваційні технології, зокрема blockchain, відкривають нові можливості у сфері електронного голосування. Використання цієї технології обіцяє підвищення прозорості, безпеки та ефективності виборчих процесів. Проте впровадження blockchain у цю сферу стикається з низкою правових викликів, які потребують ретельного аналізу. У статті розглядаються основні правові ризики, пов'язані з використанням технології blockchain у виборах, а також досвід міжнародної практики у їх подоланні.

Використання технології blockchain у виборчих процесах має потенціал для підвищення прозорості та надійності голосування, проте з цим пов'язаний ряд правових викликів. Однією з основних проблем є забезпечення конфіденційності виборців, оскільки структура blockchain передбачає відкритий доступ до транзакцій. Це може призвести до порушення принципу таємниці голосування, що є фундаментальним у демократичних системах. Хоча технології криптографії, такі як Zero-Knowledge Proofs, можуть вирішити це питання, у більшості країн відсутня чітка правова база для їх використання у виборчих системах[1]. Така ситуація вимагає оновлення законодавства для забезпечення прав виборців на конфіденційність. Ще однією складністю є відповідність blockchain-рішень чинному виборчому законодавству. У багатьох державах регулювання виборів передбачає фізичний контроль над бюлетенями або обов'язкове використання паперових носіїв для підрахунку голосів. Це створює юридичні перешкоди для впровадження децентралізованих систем. Крім того, стандарти ідентифікації виборців, електронного підпису чи процедури верифікації відрізняються залежно від юрисдикції. Така неоднорідність ускладнює інтеграцію сучасних технологій у виборчі процеси та вимагає уніфікації законодавства на міжнародному рівні.

Ми вважаємо, що глобальна природа blockchain додає ще більше викликів, оскільки виборчий процес зазвичай регулюється національними законами. Якщо ключові елементи інфраструктури системи знаходяться у різних країнах, це створює юридичні колізії. Наприклад, якщо сервера чи вузли мережі розташовані за межами юрисдикції країни, у якій проводяться вибори, виникає питання про те, яке законодавство застосовується для врегулювання суперечностей чи забезпечення захисту даних. Подібні ситуації вимагають не лише технологічних, але й дипломатичних рішень, які сприятимуть створенню міжнародних стандартів для використання blockchain у виборчих процесах.

Досвід міжнародної практики у впровадженні технології blockchain у виборчі процеси є цінним джерелом для аналізу можливостей та викликів, пов'язаних із цією інновацією. Естонія, одна з найбільш цифровізованих кра-

їн світу, стала піонером у використанні blockchain у виборчій сфері. У рамках пілотного проєкту в 2017 році ця технологія використовувалася для підвищення надійності обробки голосів та забезпечення прозорості виборів. Водночас ключовими викликами для країни стали питання захисту персональних даних та адаптація нових технологій до вже існуючої інфраструктури. Естонія довела, що створення чіткої нормативної бази, яка підтримує інновації, є фундаментальним аспектом успішного впровадження подібних систем[2]. Швейцарія також активно експериментує з blockchain у виборчих процесах, зокрема на рівні місцевих референдумів. Влада країни зробила акцент на розробці спеціалізованого законодавства, яке враховує особливості децентралізованих рішень. Це дозволяє створити правову основу, яка відповідає як вимогам конфіденційності, так і необхідності забезпечення прозорості. Досвід Швейцарії показує, що для інтеграції технології blockchain потрібен структурований підхід, який включає чітке визначення правового статусу учасників виборчого процесу та забезпечення технологічної безпеки. У Сполучених Штатах використання blockchain для голосування вперше відбулося у Західній Вірджинії у 2018 році. Цей експеримент показав важливість належного технічного аудиту системи та підкреслив загрози, пов'язані з кібербезпекою[3]. Одним із головних уроків стало усвідомлення необхідності впровадження резервних механізмів, які можуть забезпечити достовірність результатів голосування у разі технічних проблем чи зловмисних атак. Американський досвід також наголошує на необхідності залучення незалежних експертів для оцінки надійності та захищеності систем, що сприяє підвищенню довіри до таких інноваційних підходів у виборах.

Ми притримуємося позиції, що сіжнардна практика демонструє, що успішне впровадження blockchain у виборчі системи залежить не лише від технологічних рішень, але й від чіткої правової стратегії, яка враховує специфіку та ризики, пов'язані з використанням децентралізованих технологій.

Отже, впровадження blockchain у сферу електронного голосування є перспективним, але водночас ризикованим напрямом. Основними правовими викликами є забезпечення конфіденційності, відповідність нормативним актам та вирішення питань юрисдикції. Міжнародний досвід свідчить про важливість створення прозорої та адаптованої правової бази, яка враховує специфіку технології. Для успішної інтеграції blockchain у виборчі системи необхідно забезпечити правову визначеність, технологічну безпеку та залучення незалежних експертів.

Список використаних джерел:

1. Бараненко Є. О. Блокчейн, як варіант захисту даних. Застосування інформаційних технологій у діяльності правоохоронних органів. МВС України. Харків. ХНУВС. 2021. С. 15-17.
2. Беляєва Є. Г. Технологія blockchain як засіб захисту персональних даних. Протидія кіберзлочинності та торгівлі людьми. МВС України. Харків. ХНУВС. 2020. С. 132-134.
3. Петченко М.В., Данилейко Г.М. Блокчейн в економічній безпеці банківського сектора. Авіація, промисловість, суспільство : матеріали I Міжнар. наук.-практ. конф., присвяч. 60-річчю КЛК ХНУВС. Харків. ХНУВС. 2020. Ч. 2. С. 368 - 370.