

СИСТЕМА Е-ВИБОРІВ В УНІВЕРСИТЕТІ НА ОСНОВІ БЛОКЧЕЙНУ

Електронне урядування – спосіб організації державної влади за допомогою систем локальних інформаційних мереж та сегментів глобальної інформаційної мережі, що забезпечує функціонування органів влади в режимі реального часу та робить максимально простим і доступним щоденне спілкування з ними громадян, юридичних осіб, неурядових організацій. Головною складовою електронного урядування є електронний уряд – єдина інфраструктура міжвідомчої автоматизованої інформаційної взаємодії органів державної влади та органів місцевого самоврядування з громадянами та суб'єктами господарювання. Він не є доповненням або аналогом традиційного уряду, а лише визначає новий спосіб взаємодії на основі активного використання інформаційно-комунікаційних технологій (ІКТ) з метою підвищення ефективності надання державних послуг. На сьогодні в світі поширені дві основні моделі електронного урядування - e-Government 1.0 та e-Government 2.0.

Складові:

- е-уряд;
- е-медицина;
- е-телефонія;
- е-законодавство;
- е-зайнятість;
- е-освіта;
- е-бібліотека;
- е-банк;
- е-демократія;
- е-кадастр;
- е-телебачення;
- е-транспорт;

Розвиток інформаційного суспільства в Україні передбачає цілеспрямовану узгоджену діяльність всіх органів державної влади та органів місцевого самоврядування. Державна політика у сфері розвитку інформаційного суспільства та електронного урядування базується на наступних нормативно – правових джерелах (із змінами та доповненнями):

- Конституція України;
- Закон України "Про електронні документи та електронний документообіг" від 22.05.2003 № 851-IV;
- Закон України "Про електронний цифровий підпис" від 22.05.2003 № 852 IV;
- Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" від 09.01.2007 № 537-V;
- Закон України "Про доступ до публічної інформації" від 13.01.2011 № 2939-VI;
- Закон України "Про адміністративні послуги" від 06.09.2012 № 5203-VI;
- Закон України "Про захист персональних даних" від 01.06.2010 № 2297-VI;
- Стратегія сталого розвитку "Україна – 2020", схвалена Указом Президента України від 12.01.2015 № 5/2015;
- Концепція розвитку електронного урядування в Україні, затверджена розпорядження Кабінету Міністрів України від 13.12.2010 № 2250-р;
- Розпорядження Кабінету Міністрів України від 05.04.2012 № 220-р "Про схвалення плану дій з впровадження в Україні Ініціативи "Партнерство "Відкритий Уряд";

- Постанова Кабінету Міністрів України від 18.07.2012 № 670 "Деякі питання електронної взаємодії органів виконавчої влади";
- Розпорядження Кабінету Міністрів України від 15.05.2013 № 386-р "Про схвалення Стратегії розвитку інформаційного суспільства в Україні";
- Розпорядження від 11.09.2013 № 718-р "Про затвердження плану заходів щодо створення Єдиного державного порталу адміністративних послуг";

У вузькому сенсі, під електронним голосуванням мається на увазі Інтернет-голосування. Респондент (виборець) одержує на відповідному сайті електронний бюлетень (форму для голосування з варіантами можливих відповідей) і голосує, позначаючи оптимальний для себе варіант відповіді.

Термін Інтернет-голосування також охоплює різні форми вивчення громадської думки, починаючи зі сприяння у визначенні переможців конкурсів і закінчуючи політичними виборами та референдумами, що проводяться за допомогою мережи Інтернет. Один із найвідоміших в Україні прикладів визначення рейтингу споживчих уподобань за допомогою Інтернет-голосування є конкурс «Фаворити Успіху».

Справжність електронного бюлетеню під час Інтернет-голосування досягається, наприклад, за рахунок приватних реєстраційних даних користувача, або непомітних користувачу підписів у вигляді ідентифікаційної мережевої адреси та параметрів пристрою і програмного забезпечення, за допомогою якого здійснюється голосування. У досконаліших системах, що мають гарантувати ідентичність користувача та його бюлетеню, використовуються приватні цифрові підписи користувача чи навіть відбитків пальців. Важливою проблемою є збереження таємниці голосування через Інтернет. Крім того, центри голосування повинні передбачати заходи з попередження різноманітних маніпуляцій з електронними бюлетенями і відвертанню хакерських атак. Має особливе значення в межах діяльності електронного уряду.

Вимоги до систем таємного голосування:

Обов'язкові:

- ніхто, крім голосуючого, не повинен знати його вибір
- тільки легітимні учасники можуть проголосувати, і до того ж тільки один раз
- рішення голосуючого не може бути таємно або явно кимось змінено (крім, можливо, їм самим)

Бажані:

- кожен легітимний учасник може перевірити, чи правильно зарахований його голос
- кожен легітимний учасник може передумати і змінити свій вибір протягом певного періоду часу
- система повинна бути захищена від продажу голосів виборцями [22]
- в разі, якщо голос зарахований неправильно, кожен легітимний учасник може повідомити про це системі, не розкриваючи своєї анонімності [23]
- неможливо відстежити, звідки дистанційно проголосував виборець
- аутентифікація оператора
- можна дізнатися, хто брав участь у голосуванні, а хто - ні
- підтримання системи не повинно вимагати багато ресурсів
- система повинна бути відмовостійкістю у разі технічних несправностей (втрата електроживлення), ненавмисних (втрата виборцем ключа) і злочинних (навмисна видача себе за іншого виборця, DoS / DDoS) атак

Блокчейн, тобто ланцюжок блоків транзакцій – розподілена база даних, яка підтримує перелік записів, так званих блоків, що постійно зростає. База захищена від підробки та переробки. Кожен блок містить часову мітку та посилання на попередній блок хеш дерева.

Блок транзакцій – спеціальна структура для запису групи транзакцій в системі Біткоїн та аналогічних їй. Щоб транзакція вважалася достовірною («підтверженою»), її формат і підписи повинні перевірити і потім групу транзакцій записати в спеціальну структуру – блок.

Інформацію в блоках можна швидко перевірити. Кожен блок завжди містить інформацію про попередній блок. Усі блоки можна вибудувати в один ланцюжок, який містить інформацію про всі вчинені коли-небудь операції з біткоїнами. Перший блок в ланцюжку – первинний блок (англ. genesisblock) – розглядається як окремий випадок, оскільки в нього відсутній материнський блок.

Розподілена база даних Blockchain формується як безперервно зростаючий ланцюжок блоків з записами про всі транзакції. Копія бази даних або її частини одночасно зберігаються на безлічі комп'ютерів та синхронізуються відповідно до формальних правил побудови ланцюжка блоків. Інформація в блоках не шифрована і доступна у відкритому вигляді, однак захищена від змін криптографічно через хеш-ланцюжок.

Найчастіше умисна зміна інформації в будь-якій з копій бази або навіть в досить великій кількості копій не буде визнана істинною, оскільки не відповідатиме правилам. Деякі зміни можуть бути прийнятні, якщо будуть внесені в усі копії бази (наприклад, видалення кількох останніх блоків через помилку в їхньому формуванні).

Ідея полягає в тому, щоб застосувати для збереження та перевірки голосів виборців деякі з блокчейн-технологій, що забезпечить непідробність, анонімність та достовірність інформації.

Список використаних джерел

1. Доступ до інформації та електронне урядування / авт.-упоряд. М. С. Демкова, М. В. Фігель. – К.
2. Клименко, І. В. Технології електронного врядування : Навчальний посібник / І. В. Клименко, К. О. Линьов. – Київ : Вид-во ДУС, 2006. – 225 с.
3. Cranor, Lorrie Faith Electronic voting: computerize dpolls may save money, protect privacy (англ.). – ACM NewYork, NY, USA. Satoshi, 2008, с. 2-3

Науковий керівник: Гужва В.М., к.е.н., професор кафедри інформаційних систем в економіці