2. S. Rahimipour, R. Moeinfar, S. M Hashemi. Traffic prediction using a self-adjusted evolutionary neural network, J. Mod. Transport. 27, (2019), 306–316. http://dx.doi.org/10.1016/j.trc.2015.02.2019.
3. A. Emami, M. Sarvi, S.A. Bagloee. Using Kalman filter algorithm for short-term traffic flow prediction in a connected vehicle environment, J. Modern Transport. 27, (2019), 222 – 232. http://dx.doi.org/10.1155/2017/8241932.
4. A. Pompigna, F. Rupia. Comparing practice-ready forecast models for weekly and monthly fluctuations of average daily traffic and enhancing accuracy by weighting methods, Journal of Traffic and Transportation Engineering 5 (English Edition), 5, (2018), 239-253.

УДК 004.8

Руденко А.О., студент 6 курсу спеціальності ПНК-51 «Професійна освіта. Комп`ютерні технології»
Молчанова Е.Ю., канд., екон. наук, доцент доцент кафедри міжнародного менеджменту, Київський національний торговельно-економічний університет

ПРОБЛЕМА ЗАХИСТУ СИСТЕМ ОНЛАЙН ГОЛОСУВАННЯ

Київський національний університет будівництва і архітектури, м. Київ

Проблема розробки досконалих систем голосування з використанням мережі Інтернет стає все більш актуальною протягом останніх двох десятиріч, хоч різні прошарки суспільства в різних країнах мають різні уявлення щодо критеріїв досконалості цих систем.

Серед причин відсутності прогресу в галузі Інтернет голосування вказується, що ризики і негативні наслідки від фальсифікацій під час виборів можуть бути набагато значнішими, ніж під час електронної комерції.

Більшість експертів приходять до висновку, що жодна з існуючих систем для голосування через мережу Інтернет в повній мірі не відповідає наведеним вище вимогам. Однією із основних перешкод щодо забезпечення відповідності цим вимогам є труднощі з отриманням довіри виборців щодо неупередженого підрахунку голосів і збереження таємниці їх волевиявлення. Іншими словами, система голосування має бути побудована таким чином, щоб не залишалось сумнівів щодо відсутності можливості викривлення результатів волевиявлення або розкриття таємниці голосів. У тому числі, що суттєво, і з боку адміністраторів системи, що мають найвищі права доступу до її інформаційних ресурсів.

Наявність хоч однієї непрозорої процедури є підставою для недовіри і дискредитації системи. Тільки повна прозорість виконання узгоджених Законом виборчих процедур і контрольованість усіх без виключення шляхів доступу до

критичної інформації з боку будь-якої зацікавленої особи, що знаходиться у будь-якому місці, на усіх етапах роботи системи голосування у реальному часі є основною передумовою подолання недовіри виборців. Так що функціональний профіль захищеності інформаційних ресурсів системи дистанційного голосування має включати, поряд з послугами гарантованого захисту від порушень конфіденційності та цілісності, ще й послуги для забезпечення повноцінного громадського контролю. Під повноцінним мається на увазі контроль, проведення якого не залишає жодних сумнівів щодо точності виконання сервером усіх запрограмованих дій.

Бажано, щоб система голосування була побудована таким чином, щоб у виборців не залишалось жодного сумніву щодо будь-якої можливості викривлення результатів їх волевиявлення або розкриття таємниці їх голосу. Тільки повна прозорість із можливістю проконтролювати точність дій на всіх етапах роботи системи голосування в реальному часі будь-якою зацікавленою особою здатна подолати недовіру виборців. Саме такі властивості повинна мати система Інтернет голосування, яка б заслуговувала на довіру виборців, бо наявність хоч однієї непрозорої процедури є підставою для недовіри і дискредитації системи. Це означає, що кожен елемент системи, включаючи підсистему забезпечення інформаційної безпеки, повинен відповідати вимогам прозорості з точки зору можливості контролю за його роботою. Слід зауважити, що відкритість системи не є перешкодою для захисту від загроз зловмисників, а навпаки, відкриті системи мають більше шансів бути краще захищеними через можливість залучення до участі у їх перевірці і вдосконаленні необмеженої кількості фахівців. Багаторічна історія створення систем електронного голосування зі слів самих розробників свідчить про те, що на кожну чергову ідею розробників щодо захисту системи, через деякий час знаходяться зловмисники, які здатні подолати захист.

Для досконалого захисту сервера від шкідливого впливу дій зловмисників достатньо обмежити доступ для всіх користувачів, крім адміністратора, таким чином, щоб не існувало можливості заподіяти шкоду. Дії адміністратора можна обмежити на рівні прав доступу і забезпечити над ними повноцінний контроль. Ті дії адміністратора, які потребують права повного доступу, виконуються на етапі підготовки сервера до встановлення і запуску прикладного програмного забезпечення (ПЗ).

Будь-яка система голосування в Інтернеті повинна працювати таким чином, щоб виборці та спостерігачі могли перевірити результат, незалежно від використовуваного програмного забезпечення - це називається "повна перевірка". Таким чином, виборці можуть бути впевнені, що їхні голоси були записані, оскільки вони були віддані, і що всі голоси були відраховані правильно.

Незважаючи на ці побоювання, електронне та дистанційне голосування продовжує розвиватися. Оскільки більша частина населення регулярно користується Інтернетом, електронне та віддалене голосування стає стимулом для більшої участі в демократії.

Для того, щоб унеможливити фальсифікацію інтернет голосувань потрібно використовувити передові технології кібер захисту баз даних – технологію Blockchain. Вперше технологія Blockchain була використана в децентралізованій платіжній системі – Bitcoin (https://bitcoin.org/bitcoin.pdf). Це дало змогу на практиці зрозуміти переваги нової технології.

На данний момент Blockchain є однією з найбільш обговорюваних і в своєму роді революційною інновацією, яка вже знайшла велику кількість застосувань в самих різних індустріях по всьому світу. Blockchain (https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD) - це децентралізована база даних, особливістю якої є незмінюваність даних і високий ступінь безпеки. Хоч багато і прирівнюють blockchain до криптовалюта, необхідно чітко усвідомлювати, що це інструмент, який використовується в самих різних напрямках, деякі з яких: зберігання і відстеження конфіденційної інформації, такі як записи пацієнтів і патентні права, розробка децентралізованих додатків, нотаріальні документи та інше.

Коли світ почав усвідомлювати можливість використання технології blockchain за рамками криптовалюта, одним з перших напрямків, які не мають відносин до грошових транзакцій, в якому дана технологія почала розвиватися - це електронне голосування. Те, що в 2019 році голосування відбувається за допомогою ручки і паперу - це свого роду аномалія. Але електронне голосування - будь то на місцевому чи національному урядовому рівні або ж в контексті корпорацій - виправдано розглядається з підозрою, оскільки результати здаються відкритими для маніпуляцій і фальсифікацій. Саме в цій області переваги прозорості та захищеності такої технології, як blockchain показує свої переваги найбільш явно. Також розвитку в даному напрямку сприяє технологія Smart Contract - комп'ютерний алгоритм, призначений для цифрової обробки, перевірки або забезпечення виконання переговорів або виконання контракту, що дозволяють виконувати надійні транзакції без третіх сторін.

Головними перевагами зберігання даних в blockchain є безпека і прозорість в порівнянні с традиційними базами даних.

У блокчейні кожна група транзакцій хешується разом із хеш-кодом попереднього блоку, і весь блокчейн буде доступний для загального доступу. Використання даної технології для цифрового голосування може фіксувати як ідентифікатор виборця, так і кандидата, а також час проведення.

Ідентифікатори виборців є загальнодоступною та приватною парою ключових слів. Виборчі дільниці здатні зберігати голоси від основного блоку для збереження прихованих підсумків до їх випуску. Кожен голос підлягає перевірці на інтелектуальному контракті, перш ніж він направляється до кандидата або за результатами голосування.

У даній системі розумний контракт полягає в тому, що кандидат дає «голосування», якщо він задовольняє певним умовам, таким як, наприклад, сума, що складається з рівно одного голосу, перевірка того, що виборча дільниця погоджується з тим, що ідентифікатор виборця дійсний, і що голосування відбулося в дійсний діапазон дат.

Поєднуючи елементи криптографічних хешей, блокчейна, розумних контрактів, багатозначних та бічних ланцюгів, можна побудувати відкриту, перевірену та анонімну систему голосування для сучасного світу.

Список використаної літератури

1. Nakamoto, S., 2008. Bitcoin: a peer-to-peer electronic cash system, November 2008 [Електронний ресурс]. – Режим доступу: https://bitcoin.org/bitcoin.pdf
2. Блокчейн (2009) / Wikipedia. [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD
3. Кечеджиян К.А. Внедрение технологии блокчейн в сферу государственного управления как актуальный мировой тренд // Закономерности и тенденции формирования системы финансовокредитных отношений: сборник статей международной научнопрактической конференции. – 2016. – С. 54–57.
4. Борисов И.Б., Журавлев В.П. Развитие электронного голосования // Журнал о выборах. – 2011. – № 3. – С. 38–43.
5. Чимаров Н.С. Правовой аспект новой технологии блокчейн-голосования: реалии и перспективы реализации // Наука сегодня: проблемы и перспективы развития: сборник научных трудов по материалам международной научно-практической конференции: в 3 частях. Научный центр «Диспут». – 2015. – С. 139–142.

УДК 004.8

Санаулла Р.Д.Х., студент 3 курсу спеціальності 113 «Прикладна математика»
Січко Т. В., к.т.н., доцент, доцент кафедри інформаційних технологій

ВИКОРИСТАННЯ ДОПОВНЕНОЇ РЕАЛЬНОСТІ В ОСВІТІ

Донецький національний університет імені Василя Стуса, м. Вінниця

Виникнення технологій віртуальної реальності пов’язують зі створенням системи Sensorama у 1960 році. Це був перший прототип, який дозволяв переглядати 3D-стереоскопічні зображення, паралельно супроводжуючи віртуальну частину стереозвуком, запахами та вітром. Цілком очевидно, що такий винахід не міг залишитися без уваги і у 1980 році з’явився новий напрям, що і отримав назву «Віртуальна реальність». У 1990 році це поняття розширилось, та з'явився термін «Доповнена реальність». На відміну від віртуальної, доповнена реальність не заміщує людині весь навколишній світ віртуальною альтернативою, а доповнює, збагачує її, додаючи поверх навколишніх предметів додаткову інформацію [1].