

Експериментальне дослідження програмної реалізації запропонованого підходу на тестових прикладах підтвердило його ефективність.

Список використаних джерел:

1. Aggarwal C.C., Reddy C.K. Data clustering. Algorithms and Applications. Cham: Springer Ltd. Publ., Switzerland, 2015. 734 p.
2. Бодянский Е.В., Струков В.М., Узлов Д.Ю. Задача оценки близости многомерных объектов анализа данных. *Управляющие системы и машины*. 2016. № 6. С. 67-72.

Одержано 19.10.2017

УДК 004.658.6

Юлія Володимирівна ТРЕГУБ,

*студентка Національного аерокосмічного університету ім.
Н. С. Жуковського «ХАІ»*

**ВИКОРИСТАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН ДЛЯ ПРОТИДІЇ
КІБЕРЗЛОЧИННОСТІ У СФЕРІ ДЕРЖАВНОГО УПРАВЛІННЯ**

З розвитком інформаційного суспільства, державні послуги зазнають великих змін і переходять до обслуговування за допомогою мережі Інтернет. Саме тому, наша держава пропонує велику кількість онлайн послуг, а саме: електронний уряд, послуги центру державного земельного кадастру, тощо. Цим державним сервісам приділяють велику увагу кіберзлочинці. Тому постає питання про адекватний захист інтересів держави у кіберпросторі.

5-го жовтня 2017 року у Верховній Раді України був прийнятий законопроект №2126а від 19.06.2015 «Про основні засади забезпечення кібербезпеки в території України».

Згідно з Законом в Україні створюється національна система кібербезпеки, як "сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного характеру, організаційних, правових, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури." [1].

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, Національний банк України, які відпо-

відно до Конституції і законів України виконують в установленому порядку основні завдання з забезпечення надійної передачі, збереження та обробки інформації.

Саме на ці структури Законом покладено забезпечення, розвиток та стає функціонування державних послуг в умовах протидії кіберзлочинцям. Одним із методів захисту даних в державних інфраструктурах є технологія блокчейн.

Блокчейн – це розподілена база даних, яка представляє собою один із способів зберігання, обробки та захисту даних і транзакцій користувача. Організована вона у вигляді ланцюга блоків інформації, у кожен з яких записана певна кількість операцій і даних з попереднього блоку [2].

Існує два види блокчейну: приватні та публічні. Приватні блокчейни - це блокчейни, в яких створення блоків централізовано, використовується технологія «докази роботи» (proof-of-work), і всі права на зчитування/запис належать одній організації. Публічні блокчейни можуть бути прочитані будь-яким користувачем, при цьому операції захищаються механізмами криптографічного верифікації, такими як доказ виконання роботи або підтвердження частки (proof-of-stake). Права тут у всіх учасників однакові, що не гарантує повноцінну конфіденційність даних [3].

Сполучення блокчейну з реальним світом забезпечується за допомогою заздалегідь запрограмованих умов і їх передачі до всіх вузлів - розумних контрактів. Звідси випливає, що необхідність в будь-якій іншій уповноваженій особі, визнаній обома сторонами, відпадає. Смарт-контракти, засновані на криптографії, забезпечують кращу безпеку, ніж традиційні контракти, засновані на праві, і зменшують ймовірність транзакційних витрат, пов'язаних з укладанням договорів і можливих судових витрат [4].

Починаючи з 2017-го року, в Україні, розвивається проект застосування блокчейну у системі державного управління на сайтах оренди та продажу державного майна, електронному самоврядуванні та земельному кадастрі. Це дозволяє підвищити ефективність державного управління; забезпечити конфіденційність даних; зробити взаємодію з державними органами простішою, швидшою та ефективнішою.

Згідно з постановою Кабінету Міністрів України від 21 червня 2017 року №688 Міністерство аграрної політики та продовольства і Державне агентство електронного урядування та Transparency International Україна розробили Державний зе-

мельний кадастр, який відтепер працюватиме на технології Blockchain [5]. Впровадження цієї технології дозволить забезпечити надійну синхронізацію даних, що унеможливить їх підробку в результаті зовнішнього втручання, гарантує прозорість, а також дасть можливість здійснювати суспільний контроль за системою.

Застосування технології блокчейн у державних установах дозволяє наблизити онлайн сервіси нашої держави до найвищих стандартів інформаційного суспільства. Наша країна активно впроваджує вказані технології. Завдяки цьому дані користувачів будуть надійно захищені від фальсифікації та несанкційного доступу зловмисника. В результаті проведеного аналізу були запропоновані шляхи впровадження технології Blockchain 2.0 для державних установ України з використанням відкритих крипто валют. Виявлені недоліки в реалізації технології блокчейн для державного земельного кадастру України, та запропоновані шляхи їх вирішення.

Список використаних джерел:

1. Конституція України: Закон від 19.06.2015 №2126а // База даних «Законодавство України»/ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657. (дата звернення 23.10.17).
2. Wikipedia.org: Блокчейн. URL: <https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD>. (дата звернення 23.10.17).
3. Profitgid.ru: «Разница между приватными и публичными блокчейнами». URL: <https://profitgid.ru/raznica-mezhdu-publicnymi-i-privatnymi-blokchejnami.html>. (дата звернення 23.10.17).
4. Wikipedia.org: Смарт контракт. URL: https://ru.wikipedia.org/wiki/Смарт_контракт. (дата звернення 23.10.17).
5. TI-Ukraine: «Державний земельний кадастр перейшов на технологію блокчейн». URL: <https://ti-ukraine.org/news/derzhavnyi-zemelnyi-kadastr-pereishov-na-tekhnohiiu-blokchein/>. (дата звернення 23.10.17).

Одержано 01.11.2017