

https://enpuir.npu.edu.ua/bitstream/handle/123456789/36094/Postol_217-220.pdf

3. Закон України «Про місцеве самоврядування» [електронний ресурс] // Офіційний сайт Верховної Ради України <https://zakon.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80#Text>

4. Лотюк О. С. Особливості механізму конституційно-правового регулювання громадянського суспільства. Вісник Вищої ради юстиції. 2013. № 1(13). С. 92-101.

5. Політологічний енциклопедичний словник / НАН України, Інститут держави і права ім. В.М.Корецького; За ред. Ю. С. Шемшученка та ін. К. : Генеза, 2004. 736 с.

6. Зарічний О. А. Взаємодія держави та громадянського суспільства через інститути участі громадян в управлінні державними справами. Європейські перспективи. 2015. № 1. С. 48-51.

Анатолій ГУЦУЛЯК, Мар'яна ГОРБАЦЬО

здобувачі освітньо-наукової програми «Менеджмент»
Західноукраїнського національного університету
Науковий керівник – д.е.н, професор, професор кафедри
менеджменту, публічного управління та персоналу, ЗУНУ
Тетяна ЖЕЛЮК

ДЕЦЕНТРАЛІЗОВАНА ІДЕНТИФІКАЦІЯ (DID) ЯК СПОСІБ ПОВЕРНЕННЯ ЦИФРОВОГО СУВЕРЕНІТЕТУ КОРИСТУВАЧАМ ІНТЕРНЕТУ

Починаючи з 1990 року концепція «знай свого клієнта» (*Know Your Client*, далі *KYC*) - стала світовим стандартом та наріжним каменем у захисті фінансового ландшафту. Процедури *KYC* з'явилися як відповідь на швидке поширення такого явища, як відмивання коштів, отриманих злочинним шляхом та різкий ріст фінансових злочинів. Теракт 11 вересня 2001 року в США додав до процедури додатково зобов'язання контролю ризиків, пов'язаних з фінансуванням тероризму і став каталізатором широкої імплементації даних правил у законодавства всіх країн світу.

У сучасній світовій практиці, *KYC* - це загальноприйнята процедура ідентифікації та верифікації даних клієнта фінансовою компанією. Даний тип перевірки використовується для підвищення довіри до фінансових операцій між учасниками

транзакцій, а також допомагає унеможливити навмисне сприяння протиправній діяльності фінансовими організаціями.

Процедура КУС складається із трьох основних блоків: ідентифікація клієнта, верифікація даних, оцінка ризиків і моніторинг [1]. З поглибленням цифровізації економіки, важливість даних перевірок стала ще очевиднішою та еволюціонувала до додаткових процедур *EDD (Enhanced Due Diligence)*, *PEP (Politically exposed person)* та ін.

Розвиток технологій, особливо машинного навчання та штучного інтелекту, однозначно пришвидшили процедури перевірок, контролю ризиків, зменшили собівартість та покращили взаємодію з користувачем. Це безумно позитивний момент, але досі залишається невирішеною фундаментальна проблема наявної системи - централізоване збереження даних. Інформація зібрана під час проходження КУС містить надзвичайно важливі чутливі персональні дані користувачів, а отже завжди буде першочерговою цілью для хакерів. Наприклад 8,2 терабайта даних (40 мільйонів карток, 3 мільйони паспортів) зібраних мобільним платіжним додатком *MobiKwik* в Індії були ймовірно викрадені зловмисником, хоча компанія пробувала це спростувати [2]. А у 2019 році хакер оприлюднив порційно документи користувачів, які він викрав у крипто біржі *Binance*. Серед документів КУС були водійські права, паспорти, відбитки пальців [3]. Ці та інші приклади свідчать про присутню вразливість в архітектурі системи.

Міжнародна спільнота - Консорціум Всесвітньої павутини (*W3C*), яка займається покращенням цілісності, безпеки та інкубації нових інтернет-технологій, представила основну архітектуру моделі децентралізованої ідентифікації (*DID*) в липні 2022 року [4]. З цього моменту дана технологія почала активно розвиватись.

DID технологія - становить фундаментальний зсув в способах управління цифровою ідентичністю користувачів в цифровому світі. *DID* ідентифікатор, який видається децентралізованою платформою приватній особі, організації є універсальним та слугує доказом права власності на цифрову унікальність. Простими словами це цифровий паспорт, який дозволяє ідентифікувати себе в інтернет павутині без передачі особистої інформації безлічі інтернет-ресурсів, виданий без використання центрального органу, такого як уряд чи приватні корпорації.

Технологія децентралізованої ідентифікації є наріжним каменем концепції Веб 3.0, який представляє зовсім нові підходи

до розвитку інтернету. Сьогодні ми знаходимось на заході існування технології Веб 2.0, де невелика кількість корпорацій контролює весь інтернет. Це створює постійні ризики і є причиною цілком виправданих побоювань урядів країн через надмірну концентрацію влади у приватних руках. *DID* спроможна повернути колись відібраний цифровий суверенітет назад в руки користувачів, що позитивно вплине на приватність, безпеку та зменшить ризики витоку даних.

Технологія *DID* разом із блокчейном та верифікованими обліковими даними (VCs) є трьома основними стовпами цифрової суверенності. Блокчейн в цій системі виконує роль децентралізованої бази даних, яка розподілена між величезною кількістю комп'ютерів у всьому світі, в якій неможливо щось змінити чи сфальсифікувати. *DID* ідентифікатори це створений користувачем цифровий паспорт, справжність якого можна перевірити швидко перевірити віддалено. Верифіковані облікові дані - паперові та оцифровані дані користувача, захищені криптографічною технологією, яка унеможливає несанкціонований доступ до них.

Основними перевагами технології для організацій є можливість миттєвої перевірки даних користувача, без необхідності зв'язуватися з емітентом цих даних (університет, державний орган), набагато нижча собівартість генерації та вищий рівень захисту облікових даних. Для користувачів перевагою є збереження права власності на свої дані та повний контроль над ними. Ключовою особливістю є обмін даними і їх перевірка без необхідності розкриття самої інформації.

Отже, потенціал використання технології дуже великий. Одночасно зі збереженням цифрової ідентичності *DID* допоможе державним та приватним організаціям покращити операційну ефективність. Ось лише декілька прикладних застосувань: контроль цифрових ліцензій в процесі імпорту/експорту товарів та швидка перевірка оригінальності документів на митниці; завдяки можливості миттєвої перевірки переходу права власності через публічні *DID* підписи покупців та продавців дозволяє ефективно використовувати в нотаріаті; з допомогою децентралізованих ідентифікаторів можна відстежувати розвиток навичок працівників компанії протягом усього їхнього життя та оцінювати їх досягнення; обмінюватись безпечно даними між медичними установами у сфері охорони здоров'я.

Список використаних джерел

1. Moin Ahmed, KYC Solution Architecture [classic]. URL: <https://creately.com/diagram/example/i80bmo0s1/kyc-solution-architecture-classic>
2. Nasdaq, Probably The Largest KYC Data Leak In History. *Demonstrates The Importance Of Bitcoin Privacy*. March 29, 2021. URL: <https://www.nasdaq.com/articles/probably-the-largest-kyc-data-leak-in-history-demonstrates-the-importance-of-bitcoin>
3. Decrypt, Hacker dumps more KYC data, piling pressure on Binance, August 8, 2019. URL: <https://decrypt.co/8286/hacker-dumps-more-kyc-documents>
4. Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations. URL: <https://www.w3.org/TR/did-core/>

Інна ДЗЕМА

здобувачка освітньо-професійної програми
«Менеджмент закладів охорони здоров'я», ЗУНУ
Науковий керівник - к.е.н, доцент
кафедри менеджменту,
публічного управління та персоналу,
ЗУНУ Ірина СМАЧИЛО

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ОЦІНЮВАННЯ РОБОТИ МЕДИЧНИХ ПРАЦІВНИКІВ

Впровадження сучасних технологій оцінювання праці медичних працівників в закладах охорони здоров'я (ЗОЗ) необхідне для чіткої диференціації обсягу, складності та якості виконаної роботи.

Проведена оцінка роботи медичних працівників надасть змогу адміністрації ЗОЗ встановити фактичне навантаження, відсоток перевиконання норми праці та визначити, яка частка роботи виконана на складному та надскладному рівні, виявити відповідність наданої медичної допомоги чинним стандартам якості.

На сучасному етапі розвитку та реформування охорони здоров'я без впровадження чіткої, прозорої, неупередженої стандартизованої системи оцінювання роботи медичних працівників неможливо провести диференційовану оплату праці,