УДК 004.056.5:343.34

Єлизавета Георгіївна БЄЛЯЄВА,
курсантка 4 курсу факультету № 4
Харківського національного університету внутрішніх справ

Петро Сергійович КЛІМУШИН,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ТЕХНОЛОГІЯ BLOCKCHAIN ЯК ЗАСІБ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

На сьогодні люди все більше і більше пов'язані з мережею Інтернет, вони не тільки шукають інформацію або спілкуються через соціальні мережі, але й вступають у правовідносини: купують різноманітні товари, користуються послугами інтернет-банкінгу, влаштовуються на роботу, і все це зазвичай супроводжується наданням персональних даних. Ризики порушень прав громадян або ускладнення їх реалізації стали можливими в сучасному світі через цифровізацію персональних даних.

До числа таких ризиків ставитися витік персональних даних більш ніж 87 мільйонів користувачів Facebook, які були використані в передвиборних кампаніях Теда Круза, Дональда Трампа, а також перед референдумом про вихід Великобританії з Європейського Союзу. Це стало переломним моментом - про необхідність захисту персональних даних заговорили буквально все і технологія блокчейн виявилася в центрі цих обговорень. Нерідко персональні дані стають об'єктом злочинів.

Метою досліджень є здійснення аналізу зарубіжного та вітчизняного досвіду використання блокчейн технологій в захисту персональних даних та визначення пріоритетних та перспективних напрямів їх подальшого застосування в Україні.

Наявність великої кількості досліджень із питань численних переваг блокчейн технологій, таких як децентралізація, анонімність, доступність, прозорість та аудитоспроможність, існування широкого спектру програмних блоків – від управління криптовалютами, фінансових послуг, управління ризиками, Інтернету речей до створення технологій

кібербезпеки, не виключає необхідності подальшого розроблення цієї теми з захисту персональних даних громадян України [1].

Зберігання даних на єдиному сервері не може бути достатньо безпечним, а отже сервер є основною вразливістю цієї системи. Крім того, важливу роль відіграє людський фактор, оскільки у більшості випадків інформація зберігається у відкритому та незашифрованому виді, недобросовісні працівники організації можуть незаконно розповсюджувати конфіденційну інформацію за певну винагороду.

Технологія блокчейн дозволить користувачам самостійно зберігати особисті дані і повністю контролювати їх передачу кому-небудь, завдяки чому необхідність сліпо довіряти корпораціям в збереженні даних просто відпаде. Персональні дані користувачів будуть зберігатися виключно на їх девайсах, а не на віддалених серверах третьої сторони. При цьому особиста інформація буде зберігатися під захистом, забезпеченої методами криптографічного шифрування. Користувачі зможуть самі вибирати кому передавати особисту інформацію, а також самостійно визначати рівень доступу до цієї інформації. Використання блокчейна дозволяє наділити користувачів повним контролем і уникнути формування централізованих сховищ персональних даних, які дуже схильні до хакерських атак [2].

Згідно дослідження проекту TAPAS в Україні діє більше ніж 135 державних реєстрів з персональними даними громадян. Серед ключових проблем дослідники виділяють дублювання даних, низький рівень взаємодії та обміну інформацією реєстрів між собою, а також відсутність законодавства, що регулює порядок ведення реєстрів.

Такий підхід призводить до збільшення фінансових видатків на утримання подібних реєстрів, а також до зобов'язання громадянина звертатись з подібною інформацією кілька разів в різні органи державної влади для отримання адміністративних послуг, які пов'язані між собою. Тобто в Україні взаємозв'язок реєстрів лишається на досить низькому рівні. Проте проблема дублювання одних і тих самих персональних даних призводить і до інших ускладнень, а саме до порушення принципу точності та достовірності персональних даних.

Важливим кроком для захисту персональних даних буде уніфікація нормативної бази в сфері державних реєстрів. Необхідно чітко визначити суб'єктів цих правовідносин та вимог до самих реєстрів. І подібна

ініціатива вже існує. Так, 10 вересня 2019 року було зареєстровано проект закону про публічні електронні реєстри за № 2110 [3].

На базі цього закону необхідно повністю переосмислити інфраструктуру функціонування державних реєстрів в Україні, та від розпорошеної, ієрархічної структури перейти до єдиного реєстру, який буде функціонувати в розподіленому вигляді.

Створення нового розподіленого державного реєстру повинно базуватися на міжнародному досвіді, він повинен містити інформацію з усіх державних реєстрів в Україні, при цьому інформація, яка буде вноситись в цей реєстр із попередніх реєстрів повинна перевірятися на достовірність з вирішенням конфлікту між персональними даними громадян.

Будь-який орган державної влади відповідно до своїх повноважень буде мати доступ відповідного рівня до тих даних, які йому необхідні для реалізації поставлених завдань. Таке розподілення рівнів доступу дозволить уникнути дублювання інформації, а також захистити персональні дані громадян від несанкціонованого втручання.

Таким чином, такий розподілений реєстр персональних даних буде не покращенням вже діючих реєстрів, а абсолютно новим інструментом і держава зможе уникнути необхідності переробки та покращення існуючих реєстрів, налагодження їх взаємодії та обміну інформацією.

Список бібліографічних посилань

1. Яковлєв Р. В. Принципи мінімізації та точності персональних даних під час використання технології розподіленого реєстру (адміністративно-правовий аспект). *ScienceRise: Juridical Science*. 2019. № 4 (10). С. 16–24.
2. Адамов О. С., Хаханов В. І., Чумаченко С. В., Абдуллаєв В. Г. Блокчейн інфраструктура для захисту кіберсистем. *Радиоэлектроника и информатика*. 2018. № 4. С. 64–85.
3. Проект Закону про публічні електронні реєстри : від 10.09.2019 № 2110 / ініціатори: М. В. Крячко, Р. В. Соха, О. П. Федієнко, Є. В. Чернєв // База даних «Законодавство України» / Верховна Рада України. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66772 (дата звернення: 25.04.2020).

Одержано 27.04.2020