Ткачук В.О., доцент кафедри фінансів та цифрової економіки, к.е.н., доц.
Грибушин Б.М., магістрант, 2 р.н., гр. ЕПМ-20, ФБСО
Державний університет «Житомирська політехніка»

Обробка персональних даних співробітників підприємства в мережі блокчейн

Активний розвиток в останні роки децентралізованих систем обробки персональної інформації ставить перед експертами все нові запитання та виклики. У зв'язку з цим наприкінці 2018 р. Commission Nationale Informatique Libertes (CNIL) надала роз'яснення щодо особливостей обробки персональних даних співробітників з використанням технології блокчейн.

Блокчейн – це своєрідна база даних, у якій дані зберігаються і розподілені між великою кількістю вузлів (комп'ютерів) та записи про які доступні всім користувачам мережі [1, с. 205]. Схематично функціонування блокчейну можна відобразити таким чином (рис. 1):

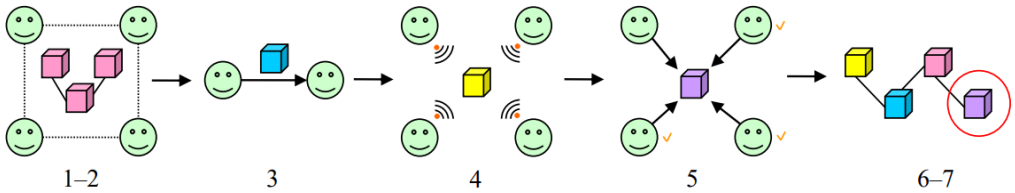

Рис. 1. Функціонування блокчейну в контексті роботи з персональними даними співробітників

Примітка: 1 – блокчейн існує у вигляді регістру в формі ланцюга з блоків інформації; 2 – кожен вузол (комп'ютер) має власну копію регістру; 3 – кожна нова транзакція представлена у вигляді блоку інформації; 4 – блок інформації доступний кожному вузлу в мережі; 5 – істинність кожного нового блоку інформації має бути підтверджена більшістю вузлів мережі; 6 – лише після підтвердження істинності блоку він додається до ланцюга регістра; 7 – після додавання нового блоку інформації до ланцюга регістра він не може бути видалений чи змінений.

З огляду на те, що провідні компанії світу активно впроваджують блокчейн у власний бізнес, можна зазначити, що використання цієї технології є доцільним і перспективним. Головними недоліками тут вбачається наступне:

– достатньо висока вартість розробки власної високонавантаженої бази даних [2, с. 35], окрім того, витрати на електроенергію для перевірки операцій на блокчейн;

– низька швидкість управління транзакціями. Зокрема, за результатами досліджень встановлено, що мережа блокчейн може управляти лише 7 транзакціями в секунду (TPS). При тому, що бренд Visa, для контексту, може обробляти 24000 TPS. Наприклад, система «підтвердження роботи/дії» Bitcoin займає близько 10 хвилин, щоб додати новий блок в блокчейн;

– конфіденційність у мережі блокчейн захищає персональні дані користувачів (у нашому випадку співробітників підприємства) від «хаків» (тобто від несанкціонованого втручання в інформаційну систему підприємства зовні), проте вона також дозволяє незаконну торгівлю та діяльність;

– нові мережі блочного ланцюга піддаються атакам на 51 %. Ці напади надзвичайно важко виконати через обчислювальну потужність, необхідну для того, щоб отримати контроль над мережею блокчейн, але дослідник інформатики Дж. Бонно відзначає, що це може змінитися. У минулому році науковець опублікував звіт про те, що 51 % атак, швидше за все, збільшиться, оскільки зараз хакери можуть просто орендувати обчислювальну потужність, а не купувати все необхідне обладнання [6, с. 23].

З блокчейн програмні додатки більше не мають потреби в розгортанні на централізованому сервері: їх можна запускати в тимчасовій мережі, яка не контролюється якоюсь однією стороною. Ці додатки на основі блокчейн можуть використовуватися для координації дій великої чисельності людей, які можуть організувати свою діяльність без допомоги третьої сторони. Технологія блокчейн – це засіб, за допомогою якого люди можуть координувати спільні дії, безпосередньо взаємодіяти один з одним і керувати собою більш безпечним і децентралізованим способом [5, с. 140].

Загалом виділяють публічний та приватний види блокчейну. Публічний блокчейн повністю децентралізований. У такому блокчейні відсутні особи, які володіють контролем над ним. Будь-яка особа може бачити транзакції та надсилати власні транзакції на підтвердження. Приватний блокчейн, зі свого боку, базується на тих самих принципах, однак його адміністрування здійснюється конкретними особами або на корпоративних засадах [4, с. 211]. Для підключення до такого блокчейну необхідний дозвіл адміністратора.

Блокчейн може містити персональні дані двох типів:

1. Ідентифікуючі дані учасників мережі, зокрема їхній публічний та приватний ключ. Публічний ключ представляє собою алфавітно-цифрову послідовність символів, згенеровану для конкретного облікового запису (аканту). Він ідентифікує кожний обліковий запис у блокчейні та доступний усім учасникам мережі. Відповідно до роз'яснень CNIL, публічний ключ є персональними даними особи, однак необхідність його використання зумовлена самою архітектурою блокчейну, тому мінімізувати такі дані чи встановити обмежений строк для їх зберігання неможливо. Приватний ключ – це вже секретна алфавітно-цифрова послідовність символів, згенерована для конкретного облікового запису. Такий ключ використовується учасником блокчейну для управління своїм обліковим записом. Приватний ключ не відомий іншим учасникам мережі та використовується кожним учасником самостійно від власного імені, тому положення General Data Protection Regulation (GDPR) на такі дані за загальним правилом не поширюватимуться.

2. Інші персональні дані – транзакції, які надсилаються учасниками на підтвердження в мережу блокчейн, можуть містити персональні дані третіх осіб. На такі персональні дані поширюватиметься дія положень GDPR.

Для визначення ролей учасників блокчейну у контексті GDPR необхідно розрізняти два основних суб'єкти:

1) учасника блокчейну, який надсилає транзакції на підтвердження в мережу;

2) учасника блокчейну, який підтверджує в мережі транзакції, надіслані іншим учасником.

Відповідно до роз'яснень CNIL учасник блокчейну, який надсилає на підтвердження транзакції, що містять персональні дані, буде виступати контролером у розумінні GDPR за умов, що такий учасник є юридичною або фізичною особою та здійснює обробку персональних даних в межах професійної чи підприємницької діяльності. На думку CNIL, учасник блокчейну, який лише підтверджує транзакції, що містять персональні дані, надіслані іншим учасником, самостійно не визначає цілей та мети обробки персональних даних, а тому повинен виступати обробником у розумінні GDPR. У такому випадку на практиці виникатимуть труднощі з дотриманням положень ст. 28 GDPR, що передбачає обов'язок контролера укласти письмовий договір з кожним обробником персональних даних.

Зважаючи на велику чисельність учасників та здебільшого анонімний характер блокчейну [3, с. 53], стає зрозумілим, що укладання договору між контролером та обробниками – учасниками блокчейну є неможливим. Технологія блокчейн зі спеціальними протоколами, що допускають різну ступінь анонімності та конфіденційності, може забезпечити захист персональних даних, допускаючи при цьому використання цих даних в додатках з штучним інтелектом. Наприклад, користувач може використовувати блокчейн з особистою інформацією про здоров'я і розкривати певні елементи цієї інформації виключно для певних цілей.

З точки зору практичного застосування у практиці діяльності сучасного підприємства у сфері захисту персональних даних, блокчейн має ряд переваг, а саме:

1) немає необхідності підтверджувати повторно, наприклад у нотаріуса, для кожної операції дійсність документів, які є верифікованими і зберігаються в учасників мережі;

2) блокчейн допомагає звірити дійсність документів у різних учасників мережі без необхідності здійснення паперового документообороту. Це суттєво економить час за операцію, оскільки не потрібно витрачати час і засоби на підготовку і доставку документів адресату, очікувати на факт перевірки документів сторонами;

3) персональну інформацію в такій розподіленій мережі неможливо загубити, а будь який її учасник може контролювати розміщенні там дані, надаючи доступ виключно за запитом.

Отже, захисту персональних даних співробітників на етапі їх обробки може сприяти використання підприємствами технології блокчейн, що представляє собою засіб, за допомогою якого люди можуть координувати спільні дії, безпосередньо взаємодіяти один з одним і керувати собою більш безпечним і децентралізованим способом. Ця технологія допускає різну ступінь конфіденційності даних і може забезпечити їх надійний захист, допускаючи при цьому використання цих даних в додатках з штучним інтелектом.

Список використаних джерел:

1. Бречко О.В., Воробець В.Є. Інституційні та організаційно-економічні детермінанти використання блокчейн-технологій у фінансовому секторі. *Інноваційна економіка*. 2020. № 3–4 [83]. С. 204–211.

2. Воржакова Ю.П., Мельник К.Г. Ефективне управління персоналом з використанням технології блокчейн – міф чи реальність? Сучасні підходи до управління підприємством: електор. зб. наук. праць, 2019. С. 27–37.

3. Воробець В. Переваги використання блокчейн-технології в умовах цифровізації фінансових інструментів. *Світ фінансів*. 2020. № 2 (63). С. 49–61.

4. Жогов В.С. Технологія блокчейн як сучасний засіб підвищення ефективності забезпечення реалізації та захисту об'єктів авторських і суміжних прав, виражених у цифровій формі. *Юридичний науковий електронний журнал*. 2020. № 2. С. 209–214.

5. Кушинова Н.Г. Запровадження та розвиток сучасних персонал-технологій в управлінні персоналом. Вісник Запорізького національного університету. 2018. № 4 (40). – С. 134–141.

6. Костюк П.П. Використання технології блокчейн для забезпечення інформаційної безпеки. *Сучасний захист інформації*. №3(43). 2020. С. 22–28.