**УКРАЇНА** **(19) UA** **(11) 157759** **(13) U**

**(51)** МПК
***G06K 19/06*** (2006.01)

**НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ДЕРЖАВНА ОРГАНІЗАЦІЯ "УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ОФІС ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ІННОВАЦІЙ"**

# (12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

**(21)** Номер заявки: **u 2024 01843**
**(22)** Дата подання заявки: **10.04.2024**
**(24)** Дата, з якої є чинними права інтелектуальної власності: **21.11.2024**
**(46)** Публікація відомостей про державну реєстрацію: **20.11.2024, Бюл.№ 47**

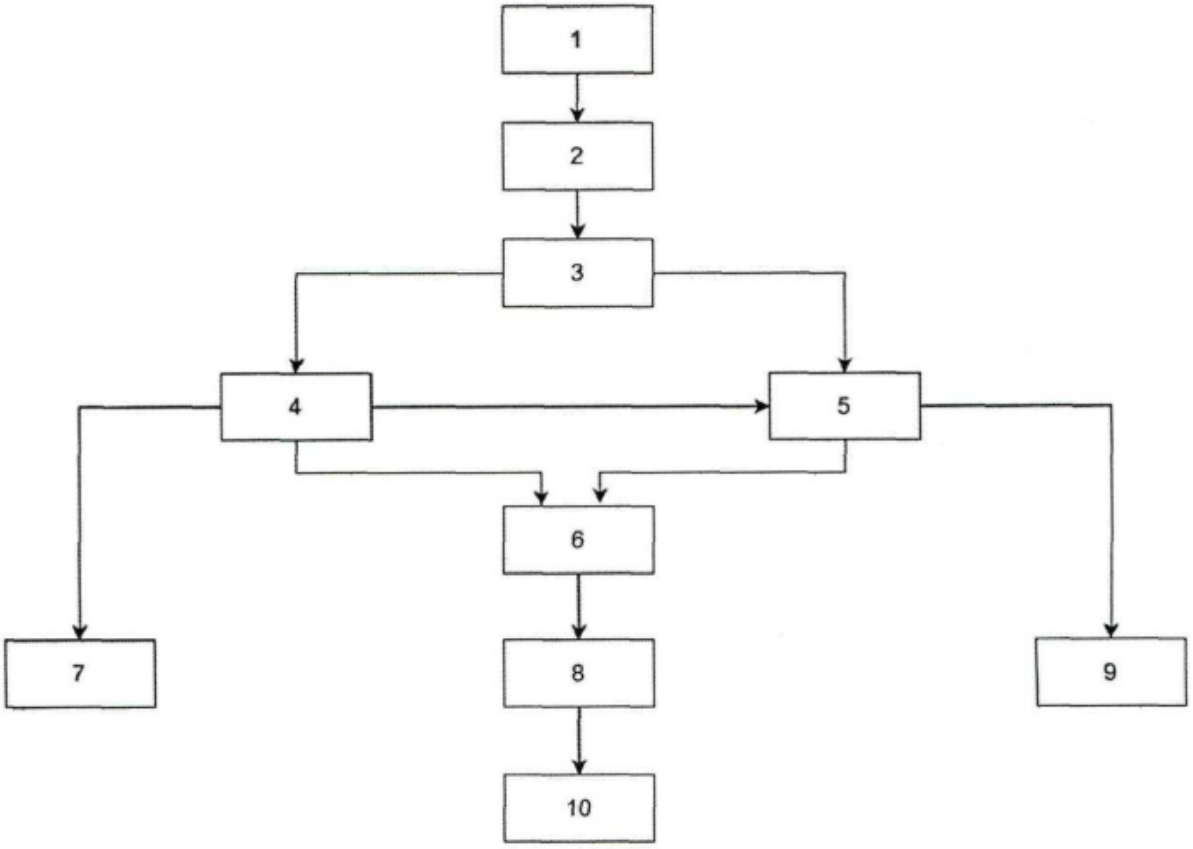
**(72)** Винахідник(и):
**Баришев Юрій Володимирович (UA),**
**Ланова Владислава Сергіївна (UA)**
**(73)** Володілець (володільці):
**ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**,
вул. Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

## (54) СПОСІБ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ ПЕРЕДАВАННЯ ДАНИХ

**(57)** Реферат:

Спосіб захисту інформації в мережах передавання даних та ідентифікації права доступу до неї полягає в тому, що інформацію після шифрування записують в базу даних, структурують її по розділах. При цьому доступ до бази даних здійснюють відкритими каналами зв'язку загального користування з виконанням криптографічних протоколів, за результатами виконання криптографічних протоколів користувачі підтверджують право доступу до розділу інформації з даним типом доступу або відхиляють це право. Після введення інформації адміністратором її обробляють в блоці сервера. Ту інформацію, що потребує підвищеного захисту конфіденційності, записують в блок передавання сервера, а інформацію невеликого обсягу записують в блок комунікації сервера. Далі інформацію розподіляють між трьома контейнерами, які включають базу даних, блокчейн та розподілене сховище даних із публічним доступом. До бази даних записують інформацію з підвищеними вимогами до захисту конфіденційності. До блокчейна записують дані для контролю цілісності інформації в базі даних та інформацію невеликого обсягу, що має підвищені вимоги до захисту цілісності та доступності даних. До розподіленого сховища даних із публічним доступом записують дані великого обсягу з підвищеними вимогами до захисту доступності.

UA 157759 U


1
2
3
4
5
6
7
8
9
10

Корисна модель належить до галузі інформаційних технологій, зокрема до області збереження інформації та передавання даних комп'ютерними мережами, переважно такими, що обслуговують, як мінімум, окрему державну галузь, таку, наприклад, як освіта, медицина і т. п.

Відомий спосіб функціонування інформаційно-виробничої системи - [деклараційний патент України на винахід № 58414, МПК H04L 9/08, H04L 9/32, опубл. 15.07.2003, бюл. № 71, 2003 р.], який полягає в тому, що всю інформацію, що занесена в банк даних, записують на зовнішні носії інформації, при цьому з вказаних даних виділяють ототожнювальні дані, які використовують для виготовлення та ідентифікації стандартизованих обов'язкових для даної галузі документів, з ототожнювальних даних виділяють інформаційні дані, які наносять на документ при його виготовленні, а при кожному сеансі зв'язку користувача з системою при сертифікації типу разового криптографічного ключа, сформованого та наданого йому на етапі реєстрації, визначають ознаку пріоритетності доступу та ознаку типу каналу, по якому користувач має право зв'язуватись з системою, протоколюють всі операції користувача і в разі вводу користувачем неправильних даних, неправильність яких визначають, порівнюючи їх з даними, що містяться у банку даних, роботу користувача з системою припиняють, визначають обсяг даних, якими користувач обмінюється з системою, тривалість обміну та кількість сеансів зв'язку користувача з системою, і при перевершенні обсягу даних і часу обміну, а також кількості сеансів зв'язку, в кожному з яких використовують визначений при реєстрації одноразовий сеансовий ключ, роботу користувача з системою припиняють.

Недоліками цього способу є недостатня захищеність сеансового ключа, що призводить до зниження рівня захисту, достовірності та цілісності інформації банка даних інформації.

Найбільш близьким до запропонованого способу є спосіб захисту інформації в мережах передачі даних та ідентифікації права доступу до неї [деклараційний патент України на винахід № 53598, МПК G06K19/06, опубл. 15.01.2003 р., бюл. № 1/2003 р.], який полягає в тому, що інформацію після шифрування одним із відомих способів записують на носії інформації, в подальшому в базу даних, структурують її по розділах, причому в кожному розділі розміщують тільки частину інформації, формують для кожного розділу тип доступу, який визначається категорією користувачів, що мають право доступу до даного розділу інформації, формують базу даних користувачів шляхом створення записів в базі даних користувачів, при цьому фіксують час реєстрації, формують унікальний ідентифікатор користувача і записують ці дані в запис користувача, записують також значення логіна та пароль користувача, припустимі мережеві адреси, з яких користувачу дозволений цей доступ, протоколи, за якими здійснюють взаємодію, період актуальності запису користувача, часовий період, протягом якого даний запис є актуальним, довідкову інформацію про користувача, створюють і записують у запис користувача криптографічні ключі та параметри криптографічних протоколів користувача, які використовують при ідентифікації та отриманні значень сеансових ключів, формують тип доступу для кожного користувача, при цьому залежно від користувача формують для нього тип доступу, який може здійснюватись виключно через захищену локальну мережу обчислювальних машин, або тип доступу, який може здійснюватись по відкритих каналах зв'язку загального користування, а право на доступ до інформації користувачеві визначають шляхом виконання даних криптографічних протоколів, що використовують надані користувачеві при реєстрації та записані в банку дані користувачів, і по результатах їх виконання підтверджують право доступу до розділу інформації з даним типом доступу, що був сформований при реєстрації даного користувача, або відхиляють це право, при підтвердженні права доступу формують спільний з користувачем сеансовий ключ обміну даними, яким зчитану інформацію шифрують і передають користувачеві, яку розшифровують за допомогою сеансового ключа, при цьому генерують новий сеансовий ключ при кожному новому сеансі обміну інформацією.

Недоліком найближчого аналога є недостатній захист цілісності та доступності даних через наявність єдиної точки відмови при зберіганні даних - бази даних.

В основу корисної моделі поставлена задача створення способу захисту інформації в мережах передачі даних, в якому за рахунок розподілу даних між трьома контейнерами, які включають базу даних, блокчейн та розподілене сховище даних із публічним доступом, підвищують цілісність та доступність інформації.

Поставлена задача вирішується за рахунок того, що у способі захисту інформації в мережах передавання даних, який полягає в тому, що інформацію після шифрування записують в базу даних, структурують її по розділах, при цьому доступ до бази даних здійснюють відкритими каналами зв'язку загального користування з виконанням криптографічних протоколів, за результатами виконання криптографічних протоколів користувачі підтверджують право доступу до розділу інформації з даним типом доступу або відхиляють це право, згідно з корисною моделлю, після введення інформації адміністратором її обробляють в блоці сервера, ту

інформацію, що потребує підвищеного захисту конфіденційності, записують в блок передавання сервера, а інформацію невеликого обсягу записують в блок комунікації сервера, далі інформацію розподіляють між трьома контейнерами, які включають базу даних, блокчейн та розподілене сховище даних із публічним доступом, до бази даних записують інформацію з підвищеними вимогами до захисту конфіденційності, до блокчейна записують дані для контролю цілісності інформації в базі даних та інформацію невеликого обсягу, що має підвищені вимоги до захисту цілісності та доступності даних, до розподіленого сховища даних із публічним доступом записують дані великого обсягу з підвищеними вимогами до захисту доступності.

На кресленні наведена схема пристрою, що реалізує спосіб захисту інформації в мережах передавання даних.

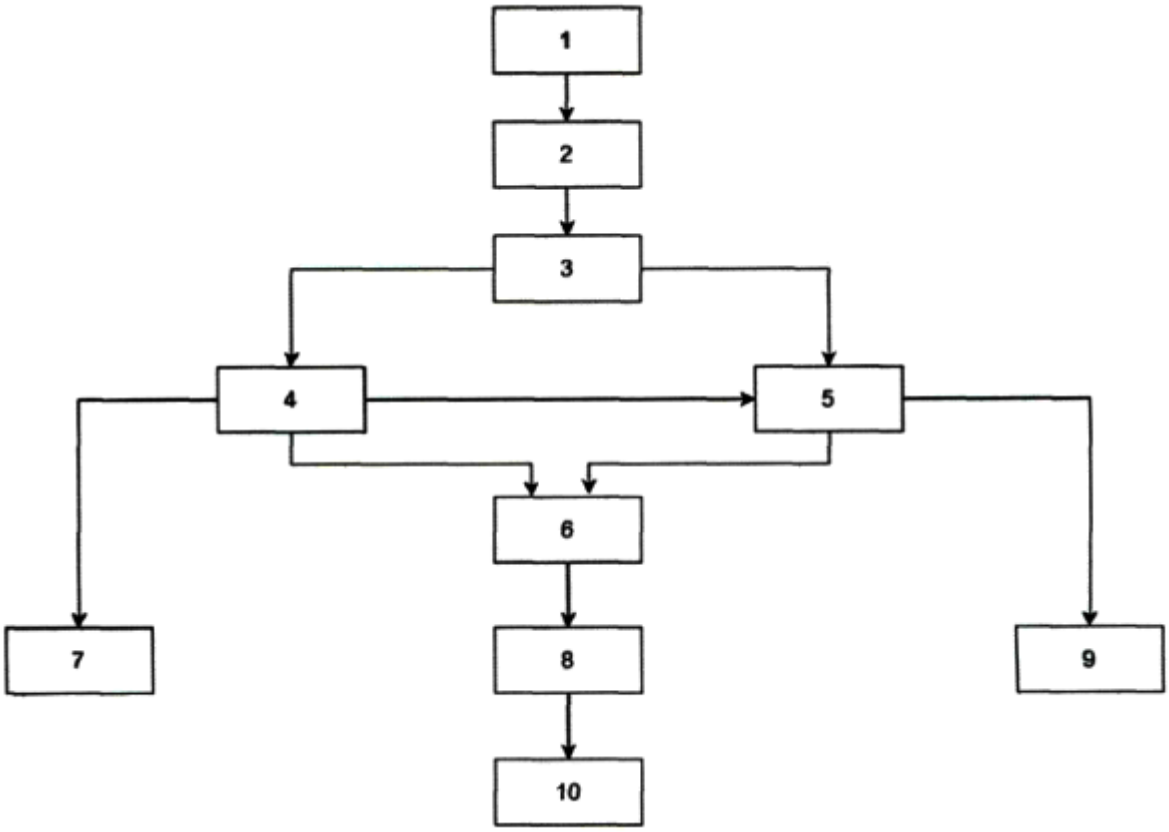
Спосіб захисту інформації в мережах передавання даних реалізується за допомогою такого пристрою: вихід блока введення інформації адміністратором 1 є входом блока сервера 2, вихід якого є входом блока з правилами класифікації сервера 3, вихід якого є входом блока передавання сервера 4, в свою чергу, виходами якого є входи блоків бази даних 7, блока клієнта 6, блока комунікації сервера 5. Вихід блока з правилами класифікації сервера 3 є входом блока комунікації сервера 5. Виходи блока комунікації сервера 5 є входами двох блоків: блока клієнта 6 та блока сховища захищеного збереження даних 9. Вихід блока клієнта 6 є входом блока криптографічних перетворень 8, вихід якого є входом блока блокчейна 10.

Спосіб захисту інформації в мережах передавання даних реалізується таким чином.

На вхід блока введення інформації адміністратором 1 подають інформацію, виражену чисельно або у вигляді байтового рядка. Інформація, що отримується на виході цього блока, є входом блока сервера 2, на якому починається обробка вхідних даних. Інформацію, що обробляють в блоці сервера 2, надсилають в блок з правилами класифікації сервера 3. Інформацію, що потребує підвищеного захисту конфіденційності, записують в блок передавання сервера 4, а інформацію невеликого обсягу - в блок комунікації сервера 5. Блок передавання сервера 4 взаємодіє з блоком бази даних 7, в який відповідно після обробки блока передавання сервера 4, надходить вихідна інформація. Вихід блока передавання сервера 4 є входом блока клієнта 6, який відповідно отримує оброблені попередньо дані та в подальшому надсилає в блок криптографічних перетворень 8, щоб ця інформація надійшла в блок блокчейна 10, у загешованому вигляді. Блок передавання сервера 4 взаємодіє з блоком комунікації сервера 5, який працює аналогічним чином над обробкою інформації та надходженням її в блок блокчейна 10. Без подальших обробок, інформація великого обсягу, після блока комунікації сервера 5 надходить в блок сховища захищеного зберігання даних 9.

## ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб захисту інформації в мережах передавання даних та ідентифікації права доступу до неї, який полягає в тому, що інформацію після шифрування записують в базу даних, структурують її по розділах, при цьому доступ до бази даних здійснюють відкритими каналами зв'язку загального користування з виконанням криптографічних протоколів, за результатами виконання криптографічних протоколів користувачі підтверджують право доступу до розділу інформації з даним типом доступу або відхиляють це право, який **відрізняється** тим, що після введення інформації адміністратором її обробляють в блоці сервера, ту інформацію, що потребує підвищеного захисту конфіденційності, записують в блок передавання сервера, а інформацію невеликого обсягу записують в блок комунікації сервера, далі інформацію розподіляють між трьома контейнерами, які включають базу даних, блокчейн та розподілене сховище даних із публічним доступом, до бази даних записують інформацію з підвищеними вимогами до захисту конфіденційності, до блокчейна записують дані для контролю цілісності інформації в базі даних та інформацію невеликого обсягу, що має підвищені вимоги до захисту цілісності та доступності даних, до розподіленого сховища даних із публічним доступом записують дані великого обсягу з підвищеними вимогами до захисту доступності.




Комп'ютерна верстка Л. Ціхановська

ДО "Український національний офіс інтелектуальної власності та інновацій", вул. Дмитра Годзенка, 1, м. Київ – 42, 01601