УКРАЇНА

(19) UA (11) 159232 (13) U

(51) МПК (2025.01)
G06F 21/31 (2013.01)
G06F 7/00

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 04391**

(22) Дата подання заявки: **10.09.2024**

(24) Дата, з якої є чинними права інтелектуальної власності: **08.05.2025**

(46) Публікація відомостей про державну реєстрацію: **07.05.2025, Бюл.№ 19**

(72) Винахідник(и):
Баришев Юрій Володимирович (UA),
Клиш Вікторія Миколаївна (UA)

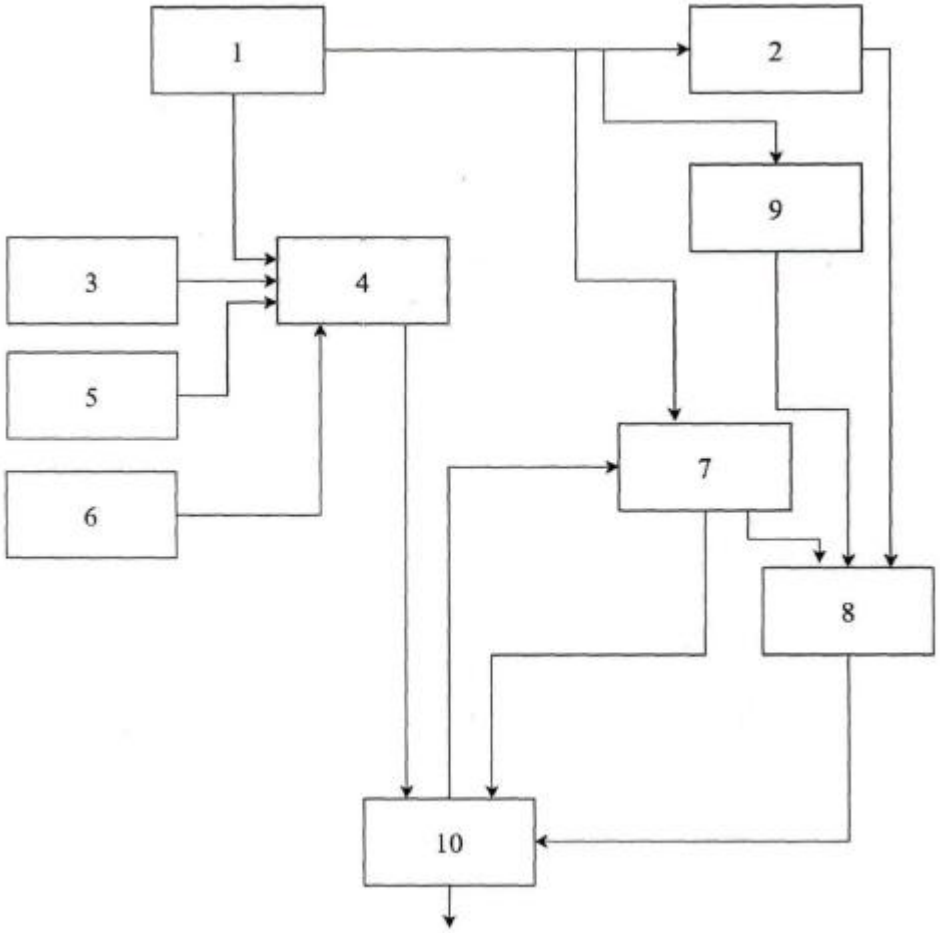
(73) Володілець (володільці):
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ,
вул. Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

(54) СПОСІБ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

(57) Реферат:

Спосіб автентифікації користувачів полягає в тому, що генерують дані доступу користувача, системою обчислюють результат гешування, користувач і система порівнюють обчислений результат зі значенням, збереженим та привласненим обліковому запису поточного користувача системи, системою дозволяють або не дозволяють доступ, геш-значення на стороні користувача обчислюють на основі параметрів робочих станцій, які отримують за допомогою пристрою введення автентифікаційних даних користувача та пристрою отримання параметрів робочої станції, відповідно, геш-значення на стороні системи отримують, використовуючи збережене геш-значення пароля користувача як ключові дані для гешування параметрів робочих станцій, з якими користувачеві дозволено працювати. Геш-значення на стороні користувача обчислюють на основі параметрів робочої станції та параметрів робочого часу, які отримують за допомогою пристрою визначення поточного часу, гешування параметрів робочих станцій, з якими користувачеві дозволено працювати, та поточного часу, на стороні системи визначають, чи поточний стан відповідає графіку роботи користувача.

UA 159232 U


1
2
9
3
4
5
6
7
8
10

Корисна модель належить до області інформаційних систем і може бути використана при організації системи безпеки в інформаційних електронних системах.

Відомий спосіб захисту даних доступу користувача системи [патент України № 9534 від 05.11.2004 р., м. кл. G06F 7/0, бюл № 10, 2005 р.], який полягає в тому, що системою генерують дані доступу користувача до системи, системою передають ідентифікатори користувачу додатком до генеральної угоди, ідентифікатори поодинці пропускають через функцію хешування, в подальшому гешування, вихідні значення ідентифікаторів складають, складене вихідне значення пропускають через інший (або той же) алгоритм функції гешування, системою обчислюють результат, значення (в подальшому геш-значення) присвоюють обліковому запису користувача у системі, видаляють початкові ідентифікатори, не зберігаючи їх у системі, для доступу до системи користувачі запитують перехід у захищений режим передачі даних, користувач і система встановлюють захищений режим, користувач передає ідентифікатори до системи, ідентифікатори поодинці пропускають через функцію гешування, вихідні значення ідентифікаторів складають, складене вихідне значення пропускають через інший алгоритм функції гешування, системою порівнюють обчислений результат зі значенням, збереженим та привласненим обліковому запису поточного користувача системи, системою дозволяють або не дозволяють доступ.

Недоліком цього способу є недостатня стійкість до атак з використанням шпигунських апаратних та програмних засобів, які можуть бути встановлені на робочій станції.

Найбільш близьким аналогом до корисної моделі є спосіб захисту даних доступу користувача системи [патент України № 116653 від 25.05.2017 р., м. кл. G06F 21/31, G06F 7/00, бюл № 10, 2017 р.], який полягає в тому, що генерують дані доступу користувача, системою обчислюють результат гешування, геш-значення присвоюють обліковому запису користувача у системі, для доступу користувачі запитують перехід у захищений режим передачі даних, користувач і система встановлюють захищений режим, порівнюють обчислений результат зі значенням, збереженим та привласненим обліковому запису поточного користувача системи, системою дозволяють або не дозволяють доступ, геш-значення на стороні користувача обчислюють на основі пароля користувача та параметрів робочих станцій, які отримують за допомогою пристрою введення автентифікаційних даних користувача та пристрою отримання параметрів робочої станції, відповідно, геш-значення на стороні системи отримують, використовуючи збережене геш-значення пароля користувача як ключові дані для гешування параметрів робочих станцій, з якими користувачеві дозволено працювати.

Недоліком найближчого аналога є те, що він не обмежує користувача в часі, протягом якого користувачеві надається доступ, що зменшує стійкість автентифікації.

В основу корисної моделі поставлена задача створення способу автентифікації користувачів, в якому за рахунок нових операцій та їх послідовності стає можливим покращення віддаленої автентифікації користувачів з урахуванням часу доступу, що призводить до підвищення стійкості.

Поставлена задача вирішується тим, що генерують дані доступу користувача, системою обчислюють результат гешування, користувач і система порівнюють обчислений результат зі значенням, збереженим та привласненим обліковому запису поточного користувача системи, системою дозволяють або не дозволяють доступ, геш-значення на стороні користувача обчислюють на основі параметрів робочих станцій, які отримують за допомогою пристрою введення автентифікаційних даних користувача та пристрою отримання параметрів робочої станції, відповідно, геш-значення на стороні системи отримують, використовуючи збережене геш-значення пароля користувача як ключові дані для гешування параметрів робочих станцій, з якими користувачеві дозволено працювати, геш-значення на стороні користувача обчислюють на основі параметрів робочої станції та параметрів робочого часу, які отримують за допомогою пристрою визначення поточного часу, гешування параметрів робочих станцій, з якими користувачеві дозволено працювати, та поточного часу, на стороні системи визначають, чи поточний стан відповідає графіку роботи користувача.

На кресленні наведена схема пристрою, що реалізує спосіб автентифікації користувачів.

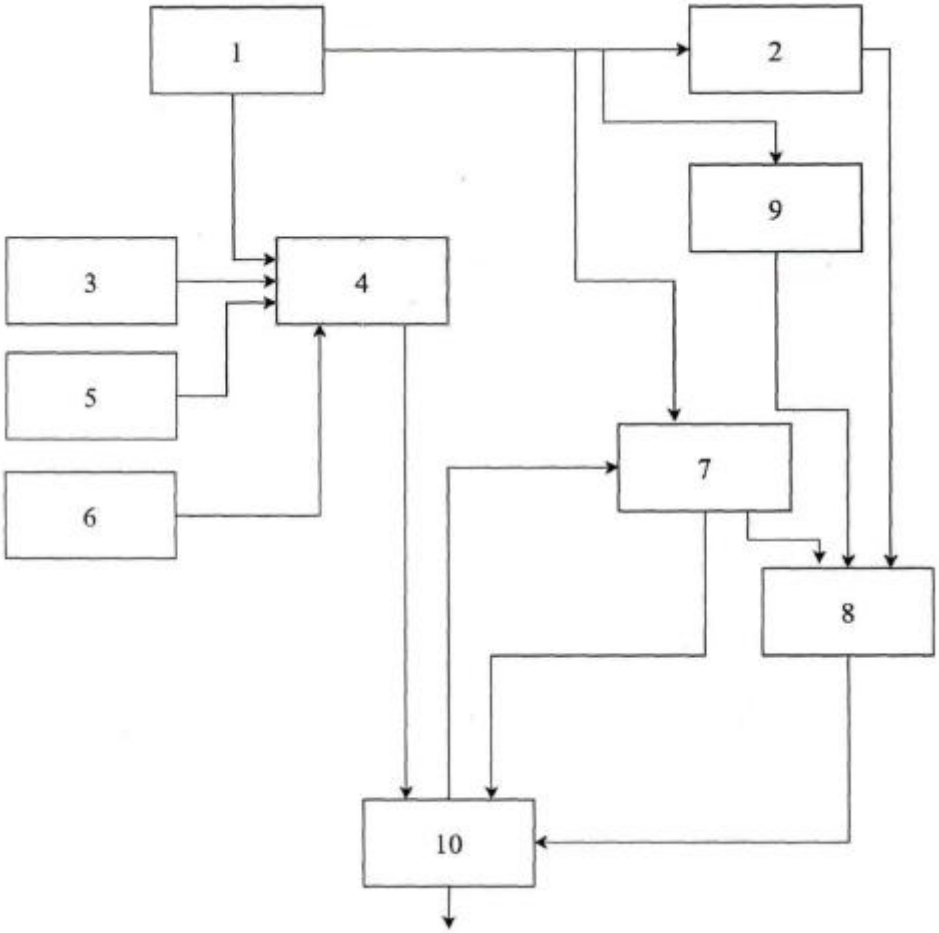
Схема містить пристрій введення автентифікаційних даних користувача 1, перший вихід якого є входом до пристрою зберігання геш-значень паролів 2, першим входом пристрою зберігання параметрів робочих станцій 7 та першим входом пристрою синхронізації часу на стороні сервера 9. Другий вихід пристрою введення автентифікаційних даних користувача 1 є першим входом першого пристрою гешування 4. Вихід пристрою зберігання геш-значень паролів 2 є другим входом другого пристрою гешування 8. Другим входом першого пристрою гешування 4 є вихід з регістру зберігання ключа 3, а третім входом є вихід з пристрою отримання параметрів робочої станції 5. Пристрій синхронізації часу на стороні користувача 6 є

четвертим входом до першого пристрою гешування 4. Перший вихід пристрою зберігання параметрів робочих станцій 7 є другим входом пристрою порівняння 10, а другий вихід є першим входом другого пристрою гешування 8. Другий вхід пристрою зберігання параметрів робочих станцій 7 є першим виходом пристрою порівняння 10. Другий вхід пристрою синхронізації часу на стороні сервера 9 є другим виходом пристрою порівняння 10. Пристрій синхронізації часу на стороні сервера 9 є третім входом до другого пристрою гешування 8. Першим входом пристрою порівняння 10 є вихід першого пристрою гешування 4, третім входом є вихід другого пристрою гешування 8. Другий вихід пристрою порівняння 10 є виходом всього пристрою.

Спосіб автентифікації користувачів виконується на пристрої таким чином. З пристрою введення автентифікаційних даних користувача 1 до пристрою зберігання геш-значень паролів 2 відправляють ідентифікатор користувача, а до першого пристрою гешування 4 - пароль. За допомогою першого пристрою гешування 4 на основі ключа, який отримують з регістру зберігання ключа 3, отримують геш-значення від результату конкатенації пароля, параметрів робочої станції, які визначають за допомогою пристрою отримання параметрів робочої станції 5, та параметрів часу, які отримують з виходу пристрою синхронізації часу на стороні користувача 6, та надсилають його до пристрою порівняння 10. Одночасно ідентифікатор користувача, який передають від пристрою введення автентифікаційних даних користувача 1 до пристрою зберігання геш-значень паролів 2 та надсилають до пристрою зберігання параметрів робочої станції 7. Водночас пристрій синхронізації часу на стороні сервера 9 отримує параметр часу від пристрою введення автентифікаційних даних користувача 1 та надсилає до другого пристрою гешування 8. Починають ітеративний процес. З пристрою зберігання параметрів робочої станції 7 отримують параметри робочої станції та надсилають їх до другого пристрою автентифікації 8. За допомогою другого пристрою гешування 8 гешують параметри робочої станції, з якою користувачеві дозволено працювати, та параметри часу, отримані з пристрою синхронізації часу на стороні сервера 9, використовуючи геш-значення пароля користувача, отримане з пристрою зберігання геш-значень паролів 2, як ключ гешування. За допомогою пристрою порівняння 10 порівнюють геш-значення, отримані від першого пристрою гешування 4 та від другого пристрою гешування 8. Якщо геш-значення збігаються, автентифікацію вважають успішною, надсилають сигнал дозволу доступу на другий вихід пристрою порівняння 10, який є виходом всього пристрою, і завершують виконання способу автентифікації користувачів. Якщо геш-значення не збігаються з першого виходу пристрою порівняння 10 надсилають запит на отримання параметрів наступної робочої станції на пристрій зберігання параметрів робочих станцій 7 і починають нову ітерацію. У випадку, коли з пристрою зберігання параметрів робочої станції 7 до другого пристрою гешування 8 було надіслано всі параметри робочих станцій, з якими користувачеві дозволено працювати, з пристрою зберігання параметрів робочої станції 7 надсилають до пристрою порівняння 10 сигнал про відсутність робочих станцій та параметрів часу на основі якого в пристрої порівняння 10 формують сигнал заборони доступу, який надсилають на другий вихід пристрою порівняння 10, який є виходом всього пристрою, і завершують виконання способу автентифікації користувачів.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб автентифікації користувачів, який полягає в тому, що генерують дані доступу користувача, системою обчислюють результат гешування, користувач і система порівнюють обчислений результат зі значенням, збереженим та привласненим обліковому запису поточного користувача системи, системою дозволяють або не дозволяють доступ, геш-значення на стороні користувача обчислюють на основі параметрів робочих станцій, які отримують за допомогою пристрою введення автентифікаційних даних користувача та пристрою отримання параметрів робочої станції, відповідно, геш-значення на стороні системи отримують, використовуючи збережене геш-значення пароля користувача як ключові дані для гешування параметрів робочих станцій, з якими користувачеві дозволено працювати, який **відрізняється** тим, що геш-значення на стороні користувача обчислюють на основі параметрів робочої станції та параметрів робочого часу, які отримують за допомогою пристрою визначення поточного часу, гешування параметрів робочих станцій, з якими користувачеві дозволено працювати, та поточного часу, на стороні системи визначають, чи поточний стан відповідає графіку роботи користувача.



Комп'ютерна верстка Л. Бурлак

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