



ДЕРЖАВНА СЛУЖБА  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ  
УКРАЇНИ

УКРАЇНА

(19) **UA** (11) **95734** (13) **U**  
(51) МПК (2015.01)  
**G06F 15/00**

## (12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2014 05377**  
(22) Дата подання заявки: **20.05.2014**  
(24) Дата, з якої є чинними права на корисну модель: **12.01.2015**  
(46) Публікація відомостей про видачу патенту: **12.01.2015, Бюл.№ 1**

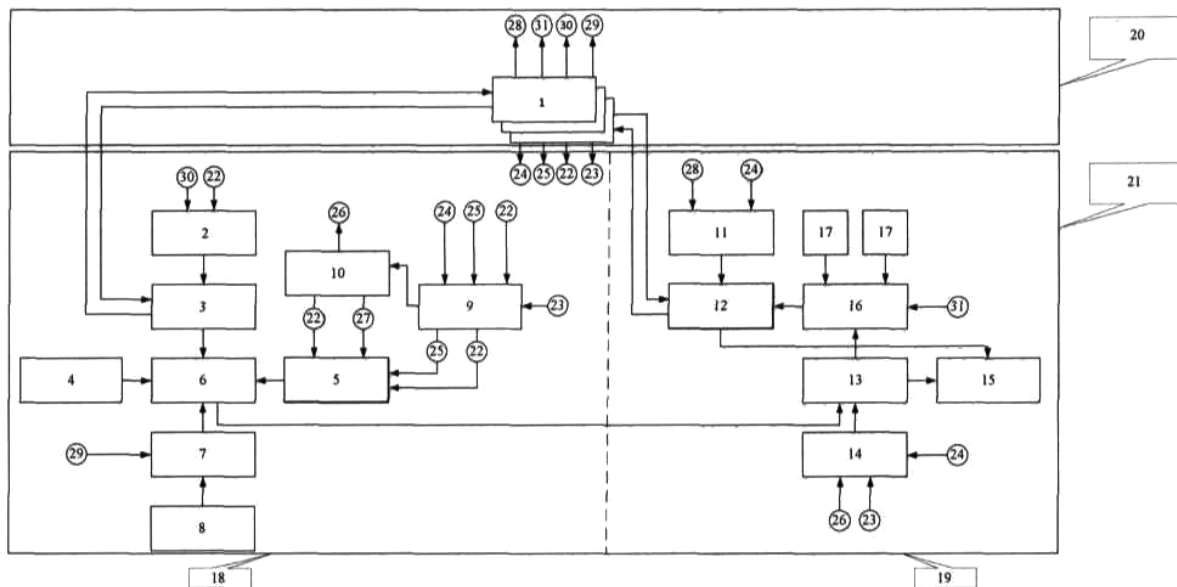
(72) Винахідник(и):  
**Данільчев Едуард Анатолійович (UA),  
Діхтяренко Микола Данилович (UA),  
Коваленко В'ячеслав Андрійович (UA),  
Ковальський Олексій Володимирович (UA),  
Кузьменко Віра Володимирівна (UA),  
Матвій Дмитро Сергійович (UA),  
Поган Олексій Михайлович (UA),  
Суховієв Олексій Васильович (UA),  
Трофимов Георгій Володимирович (UA),  
Цапко Денис Петрович (UA)**  
(73) Власник(и):  
**ТОВАРИСТВО З ОБМЕЖЕНОЮ  
ВІДПОВІДАЛЬНІСТЮ "АРТ-МАСТЕР",  
вул. Сурикова, 3 (літ. А), м. Київ, 03035 (UA)**

## (54) ПРИСТРІЙ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ АВТОМАТИЗОВАНИХ СИСТЕМ

### (57) Реферат:

Пристрій управління доступом користувачів до інформаційних ресурсів автоматизованих систем складається з серверної частини та клієнтської частини, до складу яких входять функціональні модулі у вигляді засобів обчислювальної техніки, а саме серверів, серверної частини та робочих станцій користувачів клієнтської частини, у які завантажений програмний комплекс, що забезпечує формування обчислювального середовища, у якому реалізуються алгоритми управління доступом користувачів до інформаційних ресурсів автоматизованих систем. Додатково містить модуль аналізу параметрів криптографічного алгоритму статичних ключових пар для порівняння параметрів криптографічних алгоритмів статичних ключових пар користувачів та параметрів криптографічного алгоритму статичної ключової пари серверної частини та вибору механізму узгодження ключа та модуль формування сеансових ключових пар для генерації ключової пари для кожного сеансу зв'язку та надсилання відкритого ключа згенерованої ключової пари для кожного сеансу зв'язку до серверної частини.

UA 95734 U



Корисна модель належить до галузі інформаційних технологій та інформаційної техніки, зокрема до захисту інформації в інформаційно-телекомунікаційних системах, і може бути використана при здійсненні інформаційного обміну між серверною частиною автоматизованої системи та робочими станціями користувачів - юридичних та фізичних осіб, що відповідно до наданих їм повноважень здійснюють доступ до інформаційних ресурсів, зосереджених у серверах автоматизованої системи.

Відомий пристрій управління доступом користувачів до інформаційних ресурсів автоматизованих систем (Патент RU 2439692, H04L9/32, G06F21/22, публікація 07.06.2013 р.), що вибраний як найближчий аналог. Пристрій складається з серверної частини та клієнтської частини, до складу яких входять функціональні модулі у вигляді засобів обчислювальної техніки, а саме серверів серверної частини та робочих станцій користувачів клієнтської частини, у які завантажено програмний комплекс, що забезпечує формування обчислювального середовища, у якому реалізуються алгоритми управління доступом користувачів до інформаційних ресурсів автоматизованих систем.

Кожний із функціональних модулів призначений для виконання певного набору функцій, які у сукупності складають повний цикл процедур щодо забезпечення доступу користувачів до інформаційних ресурсів автоматизованих систем, для:

- накладання електронного цифрового підпису ЕЦП та перевірки чинності сертифікатів відкритих ключів шифрування та пересилання облікових даних користувачів, ідентифікації, автентифікації та реєстрації користувачів,
- розмежування доступу користувачів до інформаційних ресурсів автоматизованих систем та
- надання користувачам, відповідно до їх повноважень, доступу до інформаційних ресурсів автоматизованих систем.

Для пересилання користувачами до серверної частини запитів/повідомлень щодо надання доступу до інформаційних ресурсів автоматизованих систем робочі станції користувачів клієнтської частини та сервери серверної частини підключенні до зовнішньої телекомунікаційної мережі.

Для забезпечення процедур доступу користувачів до інформаційних ресурсів автоматизованих систем ключовими документами та інформацією щодо чинності сертифікатів відкритих ключів сервери серверної частини та робочі станції користувачів клієнтської частини через зовнішню телекомунікаційну мережу підключені до центрів генерації, сертифікації та розповсюдження ключів, які створюють зовнішнє обчислювальне середовище, у якому реалізуються алгоритми генерації та сертифікації ключів та взаємної автентифікації користувачів та серверної частини.

Клієнтська частина містить наступні модулі.

Модуль зберігання сертифікатів відкритих ключів серверної частини.

Модуль автентифікації клієнтський для: надсилання до серверної частини сертифіката відкритого ключа ЕЦП користувача, занесення сертифіката відкритого ключа ЕЦП серверної частини до модуля зберігання сертифікатів відкритих ключів серверної частини, надсилання до центру сертифікації ключів запиту щодо чинності сертифіката відкритого ключа ЕЦП серверної частини, опрацювання отриманої від центру сертифікації ключів відповіді на запит щодо чинності сертифіката відкритого ключа ЕЦП серверної частини та генерації повідомлення про помилку у разі, коли сертифікат відкритого ключа ЕЦП серверної частини не дійсний.

Модуль формування сеансового ключа для генерації та зберігання симетричного сеансового ключа шифрування.

Модуль формування узгодженого ключа клієнтський для формування узгодженого ключа для шифрування симетричного сеансового ключа шифрування шляхом використання відкритого ключа ЕЦП серверної частини та особистого ключа ЕЦП користувача.

Модуль шифрування/дешифрування клієнтський для формування та передачі на серверну частину запиту на встановлення сеансу захищеного зв'язку з клієнтською частиною, шифрування сеансового ключа шифрування узгодженим ключем та шифрування сеансовим ключем запитів та повідомлень.

Модуль накладання/зняття ЕЦП для накладання/зняття ЕЦП при інформаційному обміні між клієнтською частиною та серверною частиною.

Модуль формування запитів для формування пакета, до складу якого входить зашифрований узгодженим ключем сеансовий ключ та зашифровані сеансовим ключем облікові дані користувача та надсилання пакета до серверної частини.

Серверна частина містить наступні модулі.

Модуль зберігання сертифікатів відкритих ключів користувачів для зберігання сертифікатів відкритих ключів ЕЦП користувачів.

Модуль автентифікації серверний для надсилання до клієнтської частини сертифіката відкритого ключа ЕЦП серверної частини, занесення сертифіката відкритого ключа ЕЦП користувача до модулю зберігання сертифікатів відкритих ключів ЕЦП користувачів, надсилання до центру сертифікації ключів запиту щодо чинності сертифіката відкритого ключа ЕЦП серверної частини, опрацювання отриманої від центру сертифікації ключів відповіді на запит щодо чинності сертифіката відкритого ключа ЕЦП користувача та генерації повідомлення про помилку у разі, коли сертифікат відкритого ключа ЕЦП користувача не дійсний.

Модуль шифрування/дешифрування серверний для дешифрування узгодженим ключем сеансового ключа шифрування та дешифрування сеансовим ключем запиту.

Модуль формування узгодженого ключа серверний для дешифрування симетричного сеансового ключа шифрування шляхом використання відкритого ключа ЕЦП користувача та особистого ключа ЕЦП серверної частини.

Модуль реєстрації користувачів, для занесення до бази даних та зберігання облікових записів користувачів.

Недоліками пристрою є:

- відсутність у користувачів можливості вибирати з власних міркувань центри генерації, сертифікації та розподілу ключів, які надаватимуть їм статичні ключові пари,

- потреба одночасно використовувати користувачем різні статичні ключові пари, отримані у різних центрах у разі необхідності отримання користувачем інформаційних послуг від різних інформаційних систем, власники яких визначили різні центри генерації, сертифікації та розподілу ключів та

- наявність у користувача відповідної кваліфікації та професійної підготовки для забезпечення реалізації прав доступу до інформаційних ресурсів системи.

Наявність недоліків пояснюється тим, що статичні ключові пари (відкритий та закритий ключі) усіма користувачами та серверною частиною повинні бути отримані від одного і того ж центру генерації, сертифікації та розподілу ключів, який визначається власником автоматизованої системи, до ресурсів якої отримують доступ користувачі.

Окрім викладеного, пристрій для забезпечення доступу користувачів до інформаційних ресурсів автоматизованої системи здійснює формування узгодженого ключа, яким шифрується сеансовий ключ. Сеансовий ключ в зашифрованому вигляді разом з зашифрованим документом передається на серверну частину автоматизованої системи, де розшифровується та використовується для розшифрування електронного документа. У разі узгодження ключів за протоколом Діффі-Геллмана, формування узгодженого ключа здійснюється за умови еквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача параметрам криптографічного алгоритму статичної ключової пари серверної частини. Таким чином користувач для забезпечення можливості доступу до ресурсів відповідної автоматизованої системи повинен отримати в визначеному власником системи центрі генерації, сертифікації та розподілу ключів статичну ключову пару, параметри криптографічного алгоритму якої еквівалентні параметрам криптографічного алгоритму статичної ключової пари серверної частини автоматизованої системи та надати до серверної частини автоматизованої системи сертифікат відкритого ключа з цієї пари. Виконання зазначеної вимоги потребує наявності у користувача відповідної кваліфікації та професійної підготовки.

Задачею корисної моделі є створення пристрою управління доступом користувачів до інформаційних ресурсів автоматизованих систем, в якому завдяки введенню до клієнтської частини додатково:

- модуля аналізу параметрів криптографічного алгоритму статичних ключових пар для порівняння параметрів криптографічних алгоритмів статичних ключових пар користувачів та параметрів криптографічного алгоритму статичної ключової пари серверної частини та вибору механізму узгодження ключа та

- модуля формування сеансових ключових пар для генерації ключової пари для кожного сеансу зв'язку та надсилання відкритого ключа згенерованої ключової пари для кожного сеансу зв'язку до серверної частини, доопрацюванню в клієнтській частині для виконання додаткового набору функцій:

- модуля формування узгодженого ключа клієнтського для надсилання користувачем до серверної частини відкритого ключа із його статичної пари ключів шифрування, формування користувачем узгодженого ключа з використанням відкритого ключа із статичної пари ключів шифрування серверної частини та особистого ключа користувача із його статичної пари ключів шифрування у разі еквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини та формування користувачем узгодженого ключа з використанням відкритого ключа

серверної частини із статичної ключової пари ключів шифрування та свого особистого ключа, що генерується у кожному сеансі зв'язку, у разі нееквівалентності параметрів криптографічного алгоритму статичної пари ключів шифрування користувача та параметрів криптографічного алгоритму статичної пари ключів шифрування серверної частини,

5 - модуля накладання/зняття ЕЦП для накладання ЕЦП на випадковий набір даних, отриманий з серверної частини та пересилання випадкового набору даних з накладеним ЕЦП до серверної частини, введенню до серверної частини додатково

10 - модуля розпізнавання ЕЦП для забезпечення єдиного інтерфейсу доступу до високорівневих функцій криптографічних бібліотек різних виробників, здійснення аналізу підписаного користувачем випадкового набору даних та перевірки його цілісності, визначення по сертифікату відкритого ключа ЕЦП виробника криптобібліотеки і, відповідно, самої криптобібліотеки, здійснення виклику визначеної криптобібліотеки, зняття ЕЦП з випадкового набору даних та визначення по ЕЦП, накладеному користувачем, центру сертифікації ключів,

15 - модуля криптобібліотек різних виробників для виконання функцій накладання/зняття ЕЦП, а також доопрацювання в серверній частині для виконання додаткового набору функцій та

20 - модуля формування узгодженого ключа серверного для надсилання до клієнтської частини відкритого ключа із статичної пари ключів шифрування, формування узгодженого ключа з використанням відкритого ключа користувача із статичної пари ключів шифрування та особистого ключа серверної частини із статичної пари ключів шифрування у разі еквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини, формування узгодженого ключа з використанням відкритого ключа, що генерується користувачем у ключовій парі для кожного сеансу зв'язку, та особистого ключа серверної частини із статичної ключової пари шифрування серверної частини, у разі нееквівалентності параметрів криптографічного алгоритму статичної ключової пари клієнта та параметрів криптографічного алгоритму статичної ключової пари серверної частини здійснюється доступ користувачів - юридичних та фізичних осіб, до інформаційних ресурсів, зосереджених у серверах автоматизованої системи. При цьому пристрій управління доступом користувачів до інформаційних ресурсів автоматизованих систем не накладає ніяких обмежень на вибір користувачем центру генерації, сертифікації та розповсюдження ключів з метою отримання послуг щодо забезпечення ключами та ключовими документами, а реалізація доступу користувача до інформаційних ресурсів автоматизованої системи не передбачає прийняття ним заходів щодо забезпечення еквівалентності параметрів криптографічного алгоритму отриманої ним статичної ключової пари параметрам криптографічного алгоритму статичної ключової пари серверної частини.

35 Поставлена задача вирішується тим, що пристрій управління доступом користувачів до інформаційних ресурсів автоматизованих систем, який складається з серверної частини та клієнтської частини, до складу яких входять функціональні модулі у вигляді засобів обчислювальної техніки, а саме серверів серверної частини та робочих станцій користувачів клієнтської частини, у які завантажений програмний комплекс що забезпечує формування обчислювального середовища, у якому реалізуються алгоритми управління доступом користувачів до інформаційних ресурсів автоматизованих систем, кожний із функціональних модулів призначений для виконання певного набору функцій, які у сукупності складають повний цикл процедур щодо забезпечення доступу користувачів до інформаційних ресурсів автоматизованих систем для накладання ЕЦП та перевірки чинності сертифікатів відкритих ключів, шифрування та пересилання облікових даних користувачів, ідентифікації, автентифікації та реєстрації користувачів, розмежування доступу користувачів до інформаційних ресурсів автоматизованих систем та надання користувачам, відповідно до їх повноважень, доступу до інформаційних ресурсів автоматизованих систем, при цьому для пересилання користувачами до серверної частини запитів/повідомлень щодо надання доступу до інформаційних ресурсів автоматизованих систем робочі станції користувачів клієнтської частини та сервери серверної частини підключені до зовнішньої телекомунікаційної мережі, а для забезпечення процедур доступу користувачів до інформаційних ресурсів автоматизованих систем ключовими документами та інформацією щодо чинності сертифікатів відкритих ключів сервери серверної частини та робочі станції користувачів клієнтської частини через зовнішню телекомунікаційну мережу підключені до центрів генерації, сертифікації та розповсюдження ключів, які створюють зовнішнє обчислювальне середовище, у якому реалізуються алгоритми генерації та сертифікації ключів та взаємної автентифікації користувачів та серверної частини, клієнтська частина пристрою містить модуль зберігання сертифікатів відкритих ключів серверної частини, 60 модуль автентифікації клієнтський для надсилання до серверної частини сертифіката

відкритого ключа електронного цифрового підпису користувача, занесення сертифіката відкритого ключа ЕЦП серверної частини до модуля зберігання сертифікатів відкритих ключів серверної частини, надсилання до центру сертифікації ключів запиту щодо чинності сертифіката відкритого ключа ЕЦП серверної частини, опрацювання отриманої від центру

5 сертифікації ключів відповіді на запит щодо чинності сертифіката відкритого ключа ЕЦП серверної частини та генерації повідомлення про помилку у разі, коли сертифікат відкритого ключа ЕЦП серверної частини не дійсний, модуль формування сеансового ключа для генерації та зберігання симетричного сеансового ключа шифрування, модуль формування узгодженого

10 ключа клієнтський, модуль шифрування/дешифрування клієнтський для формування та передачі на серверну частину запиту на встановлення сеансу захищеного зв'язку з клієнтською частиною, шифрування сеансового ключа шифрування узгодженим ключем та шифрування сеансовим ключем запитів та повідомлень, модуль накладання/зняття ЕЦП для накладання/зняття ЕЦП при інформаційному обміні між клієнтською частиною та серверною

15 частиною та модуль формування запитів для формування пакета, до складу якого входить зашифрований узгодженим ключем сеансовий ключ та зашифровані сеансовим ключем облікові дані користувача, та передачі пакета до серверної частини, серверна частина пристрою містить модуль зберігання сертифікатів відкритих ключів користувачів для зберігання сертифікатів відкритих ключів ЕЦП користувачів, модуль автентифікації серверний для надсилання до

20 клієнтської частини сертифіката відкритого ключа ЕЦП серверної частини, занесення сертифіката відкритого ключа ЕЦП користувача до модуля зберігання сертифікатів відкритих ключів користувачів, надсилання до центру сертифікації ключів запиту щодо чинності сертифіката відкритого ключа ЕЦП серверної частини, опрацювання отриманої від центру

25 сертифікації ключів відповіді на запит щодо чинності сертифіката відкритого ключа ЕЦП користувача та генерації повідомлення про помилку у разі, коли сертифікат відкритого ключа ЕЦП користувача не дійсний, модуль шифрування/дешифрування серверний для дешифрування узгодженим ключем сеансового ключа шифрування та дешифрування

сеансовим ключем запиту, модуль формування узгодженого ключа серверний та модуль реєстрації користувачів для занесення до бази даних та зберігання облікових записів користувачів. Згідно з корисної моделі клієнтська частина додатково містить модуль аналізу

30 параметрів криптографічного алгоритму статичних ключових пар для порівняння параметрів криптографічних алгоритмів статичних ключових пар користувачів та параметрів криптографічного алгоритму статичної ключової пари серверної частини та вибору механізму узгодження ключа та модуль формування сеансових ключових пар для генерації ключової пари для кожного сеансу зв'язку та надсилання відкритого ключа згенерованої ключової пари для

35 кожного сеансу зв'язку до серверної частини, а також доопрацюванні для виконання додаткового набору функцій модуль формування узгодженого ключа клієнтський для надсилання користувачем до серверної частини відкритого ключа із його статичної пари ключів шифрування, формування користувачем узгодженого ключа з використанням відкритого ключа із статичної пари ключів шифрування серверної частини та особистого ключа користувача із

40 його статичної пари ключів шифрування у разі еквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини та формування користувачем узгодженого ключа з використанням відкритого ключа серверної частини із статичної ключової пари ключів шифрування та свого особистого ключа, що генерується у кожному сеансі зв'язку, у разі

45 нееквівалентності параметрів криптографічного алгоритму статичної пари ключів шифрування користувача та параметрів криптографічного алгоритму статичної пари ключів шифрування серверної частини, модуль накладання/зняття ЕЦП для накладання електронного цифрового підпису на випадковий набір даних отриманий з серверної частини та пересилання випадкового набору даних з накладеним ЕЦП підписом до серверної частини, серверна частина додатково

50 містить модуль розпізнавання ЕЦП для забезпечення єдиного інтерфейсу доступу до високорівневих функцій криптографічних бібліотек різних виробників, здійснення аналізу підписаного користувачем випадкового набору даних та перевірки його цілісності, визначення по сертифікату відкритого ключа ЕЦП виробника криптобібліотеки і, відповідно, самої криптобібліотеки, здійснення виклику визначеної криптобібліотеки, зняття ЕЦП з випадкового

55 набору даних та визначення по ЕЦП, накладеному користувачем, центру сертифікації ключів, та модуль криптобібліотек різних виробників для виконання функцій накладання/зняття ЕЦП, а також доопрацьований для виконання додаткового набору функцій модуль формування узгодженого ключа серверний для надсилання до клієнтської частини відкритого ключа із статичної пари ключів шифрування, формування узгодженого ключа з використанням відкритого

60 ключа користувача із статичної пари ключів шифрування та особистого ключа серверної

частини із статичної пари ключів шифрування у разі еквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини, формування узгодженого ключа з використанням відкритого ключа, що генерується користувачем у ключовій парі для кожного сеансу зв'язку, та особистого ключа серверної частини із статичної ключової пари шифрування серверної частини, у разі нееквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини.

В результаті запропонованого пристрою управління доступом користувачів до інформаційних ресурсів автоматизованих систем забезпечується захищений інформаційний обмін між клієнтською та серверною частинами автоматизованої системи незалежно від того, від якого центру генерації, сертифікації та розповсюдження ключів користувач отримав статичну ключову пару, бібліотеку якого виробника він використав для накладання електронного цифрового підпису та чи еквівалентні параметри криптографічних алгоритмів статичних ключових пар користувачів параметрам криптографічного алгоритму статичної ключової пари серверної частини автоматизованої системи, доступ до якої отримують користувачі.

Суть корисної моделі пояснюється кресленням, де представлена структурна схема пристрою.

На структурній схемі позначено:

1. Центри генерації, сертифікації та розповсюдження ключів різних виробників.
2. Модуль збереження сертифікатів відкритих ключів серверної частини.
3. Модуль автентифікації клієнтський.
4. Модуль формування сеансового ключа.
5. Модуль формування узгодженого ключа клієнтський.
6. Модуль шифрування/дешифрування клієнтський.
7. Модуль накладання/зняття ЕЦП.
8. Модуль формування запитів.
9. Модуль аналізу параметрів криптографічного алгоритму статичних ключових пар.
10. Модуль формування сеансових ключових пар.
11. Модуль зберігання сертифікатів відкритих ключів клієнтів.
12. Модуль автентифікації серверний.
13. Модуль шифрування/дешифрування серверний.
14. Модуль формування узгодженого ключа серверний.
15. Модуль реєстрації клієнтів.
16. Модуль розпізнавання ЕЦП.
17. Модуль криптобібліотек, різних виробників.
18. Клієнтська частина пристрою.
19. Серверна частина пристрою.
20. Зовнішнє обчислювальне середовище.
21. Обчислювальне середовище автоматизованої системи.
22. Відкритий ключ серверної частини із статичної пари ключів шифрування.
23. Особистий ключ серверної частини із статичної пари ключів шифрування.
24. Відкритий ключ користувача із статичної пари ключів шифрування.
25. Особистий ключ користувача із статичної пари ключів шифрування.
26. Відкритий ключ користувача, що генерується у ключовій парі для кожного сеансу.
27. Особистий ключ користувача, що генерується у ключовій парі для кожного сеансу.
28. Відкритий ключ ЕЦП користувача.
29. Особистий ключ ЕЦП користувача.
30. Відкритий ключ ЕЦП серверної частини.
31. Особистий ключ ЕЦП серверної частини.

Пристрій складається з серверної частини та клієнтської частини, які підключені до зовнішньої телекомунікаційної системи та до складу яких входять функціональні модулі у вигляді засобів обчислювальної техніки - серверів та робочих станцій клієнтів.

Клієнтська частина пристрою реалізована у вигляді сукупності робочих станцій користувачів. Підключення робочих станцій користувачів до зовнішньої телекомунікаційної мережі з метою забезпечення інформаційного обміну з серверною частиною та центрами генерації, сертифікації та розповсюдження ключів забезпечується з використанням WEB-браузерів.

Серверна частина пристрою реалізована у вигляді локальної обчислювальної мережі, до складу якої входять WEB-сервери та Проху-сервери, що забезпечують управління доступом користувачів до інформаційних ресурсів, зосереджених у базах даних, забезпечення та

синхронізацію інформаційного обміну з клієнтською частиною пристрою та центрами генерації, сертифікації та розповсюдження ключів.

Персональні електронно-обчислювальні машини, які використовуються в робочих станціях клієнтської частини пристрою, обладнані 64-х розрядним процесором Intel Pentium/Celeron, підключення до зовнішньої телекомунікаційної здійснюється з використанням Інтернет-проводника Internet Explorer Browser. У складі серверної частини пристрою використовуються WEB-сервери типу Apache та MS IIS.

Програмне забезпечення, що завантажується у засоби обчислювальної техніки серверної та клієнтської частини пристрою складається з функціональних модулів, які у сукупності забезпечують виконання повного циклу функцій управління доступом користувачів до інформаційних ресурсів автоматизованої системи.

Модуль 2 реалізує функцію збереження сертифікатів відкритих ключів 28. Модуль 3 реалізує функції надсилання до серверної частини сертифікату відкритого ключа 28, занесення сертифікату відкритого ключа 30 до модулю збереження сертифікатів відкритих ключів серверної частини, надсилання до центру сертифікації ключів запиту щодо чинності сертифікату відкритого ключа 30, опрацювання отриманої від центру сертифікації ключів відповіді на запит щодо чинності сертифікату відкритого ключа 30 та генерації повідомлення про помилку у разі, коли сертифікат відкритого ключа 30 не дійсний.

Модуль 4 реалізує функцію генерації та зберігання симетричного сеансового ключа. Модуль 5 реалізує функції надсилання на серверну частину пристрою ключа 24, формування користувачем узгодженого ключа з використанням ключа 22 та ключа 25 (статичного механізму узгодження ключа) у разі еквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини, формування користувачем узгодженого ключа з використанням ключа 22 та ключа 27 (динамічного механізму узгодження ключа) у разі нееквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини.

Модуль 6 реалізує функцію формування та передачі на серверну частину запиту на встановлення сеансу захищеного зв'язку з серверною частиною, шифрування сеансового ключа узгодженим ключем, шифрування сеансовим ключем HTTP-запитів та HTTP-відповідей.

Модуль 7 реалізує функції накладання/зняття ЕЦП при інформаційному обміні між клієнтською частиною та серверною частиною, накладання ЕЦП на випадковий набір даних, отриманий з серверної частини, пересилання підписаного ЕЦП випадкового набору даних на серверну частинну.

Модуль 8 реалізує функцію формування пакета, до складу якого входить зашифрований узгодженим ключем сеансовий ключ та зашифровані сеансовим ключем облікові дані користувача та надсилання користувачем пакета до серверної частини.

Модуль 9 реалізує функцію порівняння параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини та вибору механізму узгодження ключа.

Модуль 10 реалізує функцію генерації ключової пари для кожного сеансу зв'язку та надсилання відкритого ключа згенерованої ключової пари 26 до серверної частини.

Модуль 11 реалізує функцію збереження сертифікатів відкритих ключів користувача.

Модуль 12 реалізує функції надсилання до клієнтської частини сертифіката відкритого ключа ЕЦП серверної частини та занесення сертифіката відкритого ключа ЕЦП користувача до сховища відкритих ключів користувачів, надсилання до центру сертифікації ключів запиту щодо чинності сертифікату відкритого ключа ЕЦП користувача, опрацювання отриманої від центру сертифікації ключів відповіді на запит щодо чинності сертифіката відкритого ключа ЕЦП користувача та генерації повідомлення про помилку у разі, коли сертифікат відкритого ключа ЕЦП користувача не дійсний.

Модуль 13 реалізує функцію розшифрування узгодженим ключем сеансового ключа та розшифрування сеансовим ключем HTTP-запиту.

Модуль 14 реалізує функції надсилання на клієнтську частину системи ключа 22, формування узгодженого ключа з використанням ключа 24 та ключа 23 (статичного механізму узгодження ключа) у разі еквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини, формування узгодженого ключа з використанням ключа 26 та ключа 23 (динамічного механізму узгодження ключа) у разі нееквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини.



Модуль 15 реалізує функцію занесення до бази даних та збереження облікових записів користувача.

Модуль 16 реалізує функції забезпечення єдиного інтерфейсу доступу до високорівневих функцій для всіх узгоджених з модулем розпізнавання криптобібліотек, аналізу підписаного користувачем випадкового набору даних та перевірки його цілісності, визначення по сертифікату відкритого ключа ЕЦП виробника криптобібліотеки і, відповідно, самої криптобібліотеки, вибору (виклику) необхідної криптобібліотеки, зняття ЕЦП з випадкового набору даних запиту та визначення по ЕЦП, накладеному користувачем, центру сертифікації ключів.

Модуль 17 реалізує функцію виконання високорівневих функцій криптографічних перетворень (накладення/зняття ЕЦП).

#### ФОРМУЛА КОРИСНОЇ МОДЕЛІ

15 Пристрій управління доступом користувачів до інформаційних ресурсів автоматизованих систем, який складається з серверної частини та клієнтської частини, до складу яких входять функціональні модулі у вигляді засобів обчислювальної техніки, а саме серверів, серверної частини та робочих станцій користувачів клієнтської частини, у які завантажений програмний комплекс, що забезпечує формування обчислювального середовища, у якому реалізуються алгоритми управління доступом користувачів до інформаційних ресурсів автоматизованих систем, кожний із функціональних модулів призначений для виконання певного набору функцій, які у сукупності складають повний цикл процедур щодо забезпечення доступу користувачів до інформаційних ресурсів автоматизованих систем для накладання електронного цифрового підпису та перевірки чинності сертифікатів відкритих ключів, шифрування та пересилання облікових даних користувачів, ідентифікації, автентифікації та реєстрації користувачів, розмежування доступу користувачів до інформаційних ресурсів автоматизованих систем та надання користувачам, відповідно до їх повноважень, доступу до інформаційних ресурсів автоматизованих систем, при цьому для пересилання користувачами до серверної частини запитів/повідомлень щодо надання доступу до інформаційних ресурсів автоматизованих систем робочі станції користувачів клієнтської частини та сервери серверної частини підключені до зовнішньої телекомунікаційної мережі, а для забезпечення процедур доступу користувачів до інформаційних ресурсів автоматизованих систем ключовими документами та інформацією щодо чинності сертифікатів відкритих ключів сервери серверної частини та робочі станції користувачів клієнтської частини через зовнішню телекомунікаційну мережу підключені до центрів генерації, сертифікації та розповсюдження ключів, які створюють зовнішнє обчислювальне середовище, у якому реалізуються алгоритми генерації та сертифікації ключів, а також взаємної автентифікації користувачів та серверної частини, клієнтська частина містить модуль зберігання сертифікатів відкритих ключів серверної частини, модуль автентифікації клієнтський для надсилання до серверної частини сертифіката відкритого ключа електронного цифрового підпису користувача, занесення сертифіката відкритого ключа електронного цифрового підпису серверної частини до модуля зберігання сертифікатів відкритих ключів серверної частини, надсилання до центру сертифікації ключів запиту щодо чинності сертифіката відкритого ключа електронного цифрового підпису серверної частини, опрацювання отриманої від центру сертифікації ключів відповіді на запит щодо чинності сертифіката відкритого ключа електронного цифрового підпису серверної частини та генерації повідомлення про помилку у разі, коли сертифікат відкритого ключа електронного цифрового підпису серверної частини не дійсний, модуль формування сеансового ключа для генерації та зберігання симетричного сеансового ключа шифрування, модуль формування узгодженого ключа клієнтський, модуль шифрування/дешифрування клієнтський для формування та передачі на серверну частину запиту на встановлення сеансу захищеного зв'язку з клієнтською частиною, шифрування сеансового ключа шифрування узгодженим ключем та шифрування сеансовим ключем запитів та повідомлень, модуль накладання/зняття електронного цифрового підпису для накладання/зняття електронного цифрового підпису при інформаційному обміні між клієнтською частиною та серверною частиною та модуль формування запитів для формування пакета, до складу якого входить зашифрований узгодженим ключем сеансовий ключ та зашифровані сеансовим ключем облікові дані користувача, та передачі пакета до серверної частини, серверна частина містить модуль зберігання сертифікатів відкритих ключів користувачів для зберігання сертифікатів відкритих ключів електронного цифрового підпису користувачів, модуль автентифікації серверний для надсилання до клієнтської частини сертифіката відкритого ключа електронного цифрового підпису серверної частини, занесення

сертифіката відкритого ключа електронного цифрового підпису користувача до модуля зберігання сертифікатів відкритих ключів користувачів, надсилання до центру сертифікації ключів запиту щодо чинності сертифіката відкритого ключа електронного цифрового підпису серверної частини, опрацювання отриманої від центру сертифікації ключів відповіді на запит

5 щодо чинності сертифіката відкритого ключа електронного цифрового підпису користувача та генерації повідомлення про помилку у разі, коли сертифікат відкритого ключа електронного цифрового підпису користувача не дійсний, модуль шифрування/дешифрування серверний для дешифрування узгодженим ключем сеансового ключа шифрування та дешифрування сеансовим ключем запиту, модуль формування узгодженого ключа серверний та модуль

10 реєстрації користувачів для занесення до бази даних та зберігання облікових записів користувачів, який **відрізняється** тим, що клієнтська частина додатково містить модуль аналізу параметрів криптографічного алгоритму статичних ключових пар для порівняння параметрів криптографічних алгоритмів статичних ключових пар користувачів та параметрів криптографічного алгоритму статичної ключової пари серверної частини та вибору механізму

15 узгодження ключа та модуль формування сеансових ключових пар для генерації ключової пари для кожного сеансу зв'язку та надсилання відкритого ключа згенерованої ключової пари для кожного сеансу зв'язку до серверної частини, а також доопрацювання для виконання додаткового набору функцій, модуль формування узгодженого ключа клієнтський для надсилання користувачем до серверної частини відкритого ключа із його статичної пари ключів

20 шифрування, формування користувачем узгодженого ключа з використанням відкритого ключа із статичної пари ключів шифрування серверної частини та особистого ключа користувача із його статичної пари ключів шифрування у разі еквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини та формування користувачем узгодженого ключа з

25 використанням відкритого ключа серверної частини із статичної ключової пари ключів шифрування та свого особистого ключа, що генерується у кожному сеансі зв'язку, у разі нееквівалентності параметрів криптографічного алгоритму статичної пари ключів шифрування користувача та параметрів криптографічного алгоритму статичної пари ключів шифрування серверної частини, модуль накладання/зняття електронного цифрового підпису для накладання

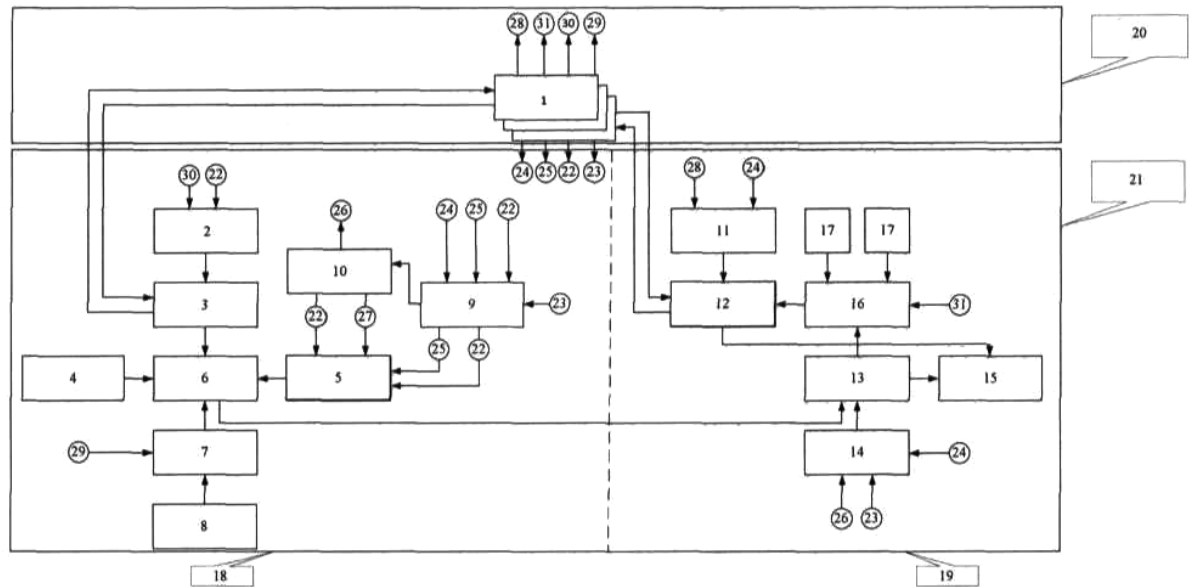
30 електронного цифрового підпису на випадковий набір даних отриманий з серверної частини та пересилання випадкового набору даних з накладеним електронним цифровим підписом до серверної частини, серверна частина додатково містить модуль розпізнавання електронного цифрового підпису для забезпечення єдиного інтерфейсу доступу до високорівневих функцій криптографічних бібліотек різних виробників, здійснення аналізу підписаного користувачем

35 випадкового набору даних та перевірки його цілісності, визначення по сертифікату відкритого ключа електронного цифрового підпису виробника криптобібліотеки і, відповідно, самої криптобібліотеки, здійснення виклику визначеної криптобібліотеки, зняття електронного цифрового підпису з випадкового набору даних та визначення по електронному цифровому підпису, накладеному користувачем, центру сертифікації ключів, та модуль криптобібліотек

40 різних виробників для виконання функцій накладання/зняття електронного цифрового підпису, а також доопрацьований для виконання додаткового набору функцій модуль формування узгодженого ключа серверний для надсилання до клієнтської частини відкритого ключа із статичної пари ключів шифрування, формування узгодженого ключа з використанням відкритого ключа користувача із статичної пари ключів шифрування та особистого ключа серверної

45 частини із статичної пари ключів шифрування у разі еквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини, формування узгодженого ключа з використанням відкритого ключа, що генерується користувачем у ключовій парі для кожного сеансу зв'язку, та особистого ключа серверної частини із статичної ключової

50 пари шифрування серверної частини, у разі нееквівалентності параметрів криптографічного алгоритму статичної ключової пари користувача та параметрів криптографічного алгоритму статичної ключової пари серверної частини.



Комп'ютерна верстка Л. Ціхановська

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601