



ДЕРЖАВНА СЛУЖБА  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ  
УКРАЇНИ

УКРАЇНА

(19) **UA** (11) **84350** (13) **U**  
(51) МПК (2013.01)  
**G06F 21/00**

## (12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

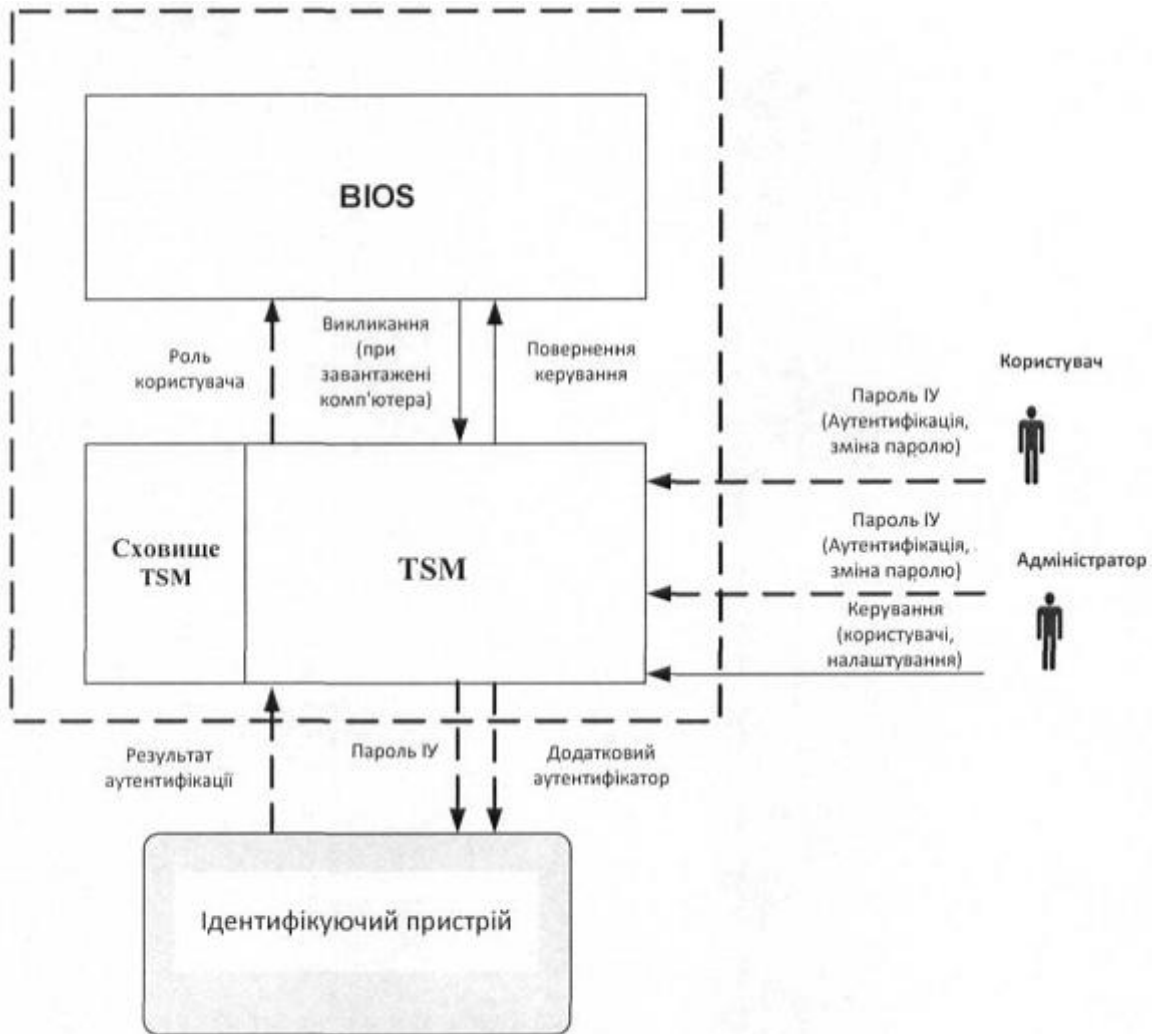
|  |                             |                     |  |
|--|-----------------------------|---------------------|--|
| (21) Номер заявки:   | <b>а 2012 12492</b>         | (72) Винахідник(и): | <b>Груздєв Сергєй Львовіч (RU/RU),<br/>Демченко Константін Олєговіч (RU/RU)</b>                                |
| (22) Дата подання заявки:                                  | <b>01.11.2012</b>           | (73) Власник(и):    | <b>ЗАКРИТОЄ АКЦИОНЕРНОЄ ОБЩЕСТВО<br/>АЛАДДІН Р.Д.,<br/>ул. Докуніна, 16, г. Москва, 129226, Росія<br/>(RU)</b> |
| (24) Дата, з якої є чинними<br>права на корисну<br>модель: | <b>25.10.2013</b>           | (74) Представник:   | <b>Зуєва Олена Миколаївна, реєстр. №249</b>  |
| (46) Публікація відомостей<br>про видачу патенту:          | <b>25.10.2013, Бюл.№ 20</b> |                     |  |

## (54) ПЕОМ ІЗ ЗАХИСТОМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

### (57) Реферат:

ПЕОМ із захистом від несанкціонованого доступу містить системну шину, базову систему введення/виведення (BIOS) і модуль безпеки TSM, що вбудовується, підключений до BIOS, причому BIOS виконано з можливістю передавати керування завантаженням ПЕОМ TSM після проходження процедури Power On Self-Test (POST). При цьому TSM містить засіб для блокування доступу до налаштувань BIOS усім, крім авторизованих адміністраторів TSM, засіб для аутентифікації користувача/адміністратора TSM, засіб для передачі керування BIOS для подальшого завантаження комп'ютера після аутентифікації користувача/адміністратора. Аутентифікація користувача/адміністратора виконується за допомогою ідентифікуючого пристрою, що підключається до системної шини ПЕОМ.

UA 84350 U



Фіг. 2

Корисна модель належить до обчислювальної техніки, а саме до довіреного завантаження комп'ютера й захисту від несанкціонованого доступу до інформації, що зберігається в персональних комп'ютерах і в комп'ютерних інформаційно-обчислювальних системах.

Використання сучасних інформаційних технологій при необхідності забезпечення конфіденційності зберігання й обробки даних є джерелом виникнення специфічних погроз із боку злоумисників. Із цим пов'язана необхідність застосування спеціальних засобів захисту інформаційних систем від несанкціонованого доступу (НСД). Штатні засоби захисту персональних ЕОМ від НСД, наприклад, використання паролів користувачів, що встановлюються за допомогою документації, що поставляється ЕОМ, гарантовано не вирішує дане завдання, тому що є можливість відключити систему контролю шляхом примусового розряду живильної батареї.

Для захисту інформації від несанкціонованого доступу широко застосовується метод шифрування інформації, що зберігається на жорсткому диску. Після завантаження ОС (системні області й файли якої не зашифровані), за допомогою спеціального або апаратно-програмного забезпечення довірених користувач може розшифрувати інформацію й одержати до неї доступ.

Багато сучасних засобів пропонують можливість шифрування системного розділу й файлів операційної системи (які в сучасних ОС можуть містити конфіденційну інформацію). Але при цьому для забезпечення завантаження ОС із жорсткого диска на ньому залишаються незашифровані області (спеціалізовані завантажники, сховища ключової інформації й ін.).

Відомі засоби програмного захисту даних (шифрування, довірене завантаження) від НСД мають недоліки, які полягають в тому, що злоумисник може змінити системні налаштування BIOS для завантаження зі свого системного диска. Що дасть злоумисникові можливість копіювання файлів, а також можливість вмонтувати шкідливе програмне забезпечення, що надалі дозволить йому одержати доступ до даних, наприклад: "клавіатурний шпигун", "троян".

Технічним результатом є підвищення ступеня захисту комп'ютера від несанкціонованого доступу до інформації.

Відповідно першого варіанта виконання ПЕОМ із захистом від несанкціонованого доступу (НСД) містить системну шину, базову систему введення/виведення (BIOS) і модуль безпеки (TSM-Trusted Security Module), що вбудовується, підключений до BIOS. BIOS виконано з можливістю передавати керування завантаженням ПЕОМ TSM після проходження процедури Power On Self-Test (POST). При цьому TSM містить засіб для блокування доступу до налаштувань BIOS усім, крім авторизованих адміністраторів TSM, засіб для аутентифікації користувача/адміністратора TSM, причому аутентифікація користувача/адміністратора виконується за допомогою ідентифікуючого пристрою (IY), що підключається до системної шини ПЕОМ, засіб для передачі керування BIOS для подальшого завантаження комп'ютера після аутентифікації користувача/адміністратора.

TSM додатково містить блок пам'яті для зберігання журналу TSM, що містить інформацію про події, викликані діями користувачів TSM, а так само про помилки, що відбулися.

TSM додатково містить засіб для виявлення несанкціонованої модифікації записів журналу.

TSM додатково містить засіб блокування доступу до ПЕОМ для всіх, крім адміністратора, у випадку виявлення несанкціонованої модифікації записів журналу.

Відповідно до другого варіанта виконання ПЕОМ із захистом від НСД містить системну шину, базову BIOS і модуль безпеки TSM, що вбудовується, підключений до BIOS. BIOS виконано з можливістю передавати керування завантаженням ПЕОМ TSM після проходження процедури POST. При цьому TSM містить засіб для блокування доступу до налаштувань BIOS усім, крім авторизованих адміністраторів TSM, засіб для аутентифікації користувача/адміністратора TSM, причому аутентифікація користувача/адміністратора виконується за допомогою IY, що підключається до системної шини ПЕОМ, засіб контролю цілісності (КЦ) програмного середовища ПЕОМ, засіб для передачі керування BIOS для подальшого завантаження комп'ютера після контролю цілісності.

Контроль цілісності виконують за допомогою порівняння контрольних сум об'єктів КЦ, причому обчислення контрольних сум об'єктів КЦ виконується за алгоритмом MD5.

Для вирішення вищезазначених і пов'язаних завдань, деякі ілюстративні аспекти описані тут у зв'язку з нижченаведеним описом і кресленнями, що додаються. Однак ці аспекти представляють лише деякі можливі підходи до застосування розкритих тут принципів і покликані охоплювати всі подібні аспекти і їхні еквіваленти. Інші переваги й ознаки новизни впливають із нижченаведеного докладного опису, наведеного разом із кресленнями.

Короткий опис креслень

На фіг. 1 представлена блок-схема роботи TSM на етапі завантаження комп'ютера.

На фіг. 2 представлена структура TSM і основні елементи, з якими він взаємодіє.

У нижченаведеному описі, з метою пояснення, численні конкретні деталі наведені для забезпечення повного розуміння корисної моделі. Однак очевидно, що нові варіанти здійснення можна здійснювати на практиці без цих конкретних деталей. В інших випадках, загальновідомі структури й пристрої показані у вигляді блок-схеми для полегшення їхнього опису.

ПЕОМ із захистом від несанкціонованого доступу, який містить модуль безпеки, що вбудовується, TSM призначений для:

захисту від НСД до комп'ютера до завантаження операційної системи (ОС),  
реєстрації подій доступу (у тому числі несанкціонованого) до комп'ютера,  
контролю цілісності (КЦ) програмного середовища комп'ютера.

TSM розташовується на материнській платі комп'ютера. Після включення комп'ютера ініціалізується BIOS. Потім викликається на виконання TSM (фіг. 1) після проходження процедури POST.

Зворотна передача керування BIOS для подальшого завантаження комп'ютера здійснюється тільки після аутентифікації користувача TSM і контролю цілісності програмного середовища комп'ютера у випадку ініціалізації функції контролю цілісності.

Після чого комп'ютер завантажується в штатному режимі: виробляється пошук завантажувального пристрою, зчитування початкового завантажника операційної системи (ОС), передача керування завантажнику ОС.

TSM взаємодіє (фіг. 2) з ідентифікуючими пристроями, у якості яких виступають, наприклад, ключі eToken або JaCarta у форм-факторі USB-ключа або смарт-карти.

Завдяки тісній інтеграції TSM з BIOS материнської плати забезпечується максимальна безпека й сумісність із усіма використовуваними апаратними засобами.

TSM забезпечує виконання наступних функцій:

ідентифікацію й аутентифікацію користувачів;

установку та зміну налаштувань TSM;

керування користувачами TSM:

реєстрацію (додавання нових) облікових записів користувачів,

зміна інформації про користувачів і налаштувань ідентифікуючих пристроїв (ІУ),

видалення облікових записів користувачів,

блокування/розблокування доступу користувачів;

зміна пароля користувача в ІУ;

контроль цілісності програмного середовища комп'ютера; реєстрацію подій TSM у журналі подій;

перегляд журналу подій;

висновок зведеної інформації про версію, налаштування, зміст сховища TSM;

захист даних TSM;

обмеження доступу до BIOS SETUP;

захист залишкової інформації.

Включення/відключення TSM

Включення/відключення TSM виробляється з BIOS SETUP.

Після включення TSM доступ до налаштувань BIOS SETUP можливий тільки Адміністраторам TSM. Це дозволяє Адміністраторові встановити необхідні налаштування BIOS, у тому числі порядок опитування завантажувальних пристроїв, і заблокувати можливість їхньої зміни для користувачів.

Так як доступ до BIOS SETUP обмежений, то відключити TSM так само може тільки Адміністратор TSM.

При відключенні TSM в BIOS SETUP присутня опція скидання вмісту пам'яті TSM, у випадку вибору якої виконується обнуління даних про зареєстрованих користувачів, підсистему контролю цілісності, журналах подій, і при повторному включенні TSM переводиться в режим ініціалізації.

Рольова модель користувачів TSM.

TSM забезпечує поділ користувачів на наступні ролі:

Адміністратор;

Користувач.

Адміністратор TSM має право на виконання наступних дій:

зміна налаштувань BIOS за допомогою BIOS SETUP;

включення/відключення TSM за допомогою BIOS SETUP;

подальше завантаження комп'ютера;

зміна налаштувань TSM;

керування користувачами TSM;

зміна пароля користувача підключеного ІУ (eToken, JaCarta);  
 перегляд журналу подій;  
 ініціалізація КЦ програмного середовища комп'ютера;  
 запит зведеної інформації про версію, налаштування, зміст сховища TSM.

5 Користувач TSM має право на виконання наступних дій: завантаження операційної системи комп'ютера;

зміна пароля користувача ІУ (eToken, JaCarta).

Ідентифікація, аутентифікація й авторизація в TSM.

Як ідентифікуючий пристрій (ІУ) виступає, наприклад, один з наступних пристроїв:

10 eToken PRO, USB-Ключ/смарт-карта з Siemens CardOS 4.01, 4.2B;

eToken PRO (Java), USB-Ключ/смарт-карта;

eToken NG-OTP;

JaCarta, USB-Ключ/смарт-карта;

iButton.

15 У випадку роботи із пристроями у виконанні смарт-карти підтримуються, наприклад, наступні зчитувачі смарт-карт:

Athena ASEDrive IIIe (USB, Keyboard);

CCID-Сумісні зчитувачі смарт-карт.

Режими ідентифікації й аутентифікації.

20 TSM підтримує два режими ідентифікації й аутентифікації:

звичайний режим;

режим роботи з корпоративними засобами ідентифікації й аутентифікації;

Умови успішної аутентифікації залежать від використовуваного режиму.

Умови аутентифікації режиму роботи з корпоративними засобами ідентифікації й аутентифікації перевіряються додатково до умов звичайного режиму.

25 Якщо умови успішної аутентифікації не виконані, подальше завантаження комп'ютера неможливе.

TSM надає Адміністраторові TSM можливість включення режиму ідентифікації й аутентифікації корпоративними засобами.

30 Звичайний режим ідентифікації й аутентифікації.

Одному користувачеві відповідає один ідентифікатор.

Аутентифікація користувачів здійснюється за допомогою пред'явлення пароля до ІУ. Кількість спроб аутентифікації обмежується залежно від політики безпеки організації, наприклад у діапазоні від 1 до 15.

35 Після перевірки пароля до ІУ TSM перевіряє наявність додаткового фактора аутентифікації на ІУ, що являє собою випадкову послідовність, збережену на ІУ й у профілі користувача в TSM. Авторизація Користувача або Адміністратора виконується відповідно до рольової моделі, описаної раніше.

Режим роботи з корпоративними засобами ідентифікації й аутентифікації.

40 У даному режимі умовою успішної аутентифікації є підтвердження факту наявності в користувача ІУ, що має унікальні для корпоративної системи ознаки.

При застосуванні умов успішної аутентифікації даного режиму застосовуються наступні обмеження:

TSM робить авторизацію відповідно до ролі Користувача;

45 TSM фіксує ідентифікатор ІУ, за допомогою якого здійснюється доступ до ресурсів комп'ютера;

використовується "твердий" режим КЦ;

функції зміни пароля ІУ недоступні.

Зміна пароля до ідентифікуючого пристрою.

50 В TSM передбачена можливість зміни пароля до ідентифікуючого пристрою користувача після проходження процедури авторизації.

Так само передбачена можливість примусової зміни пароля за замовчуванням.

Режими функціонування TSM.

TSM має наступні режими функціонування:

55 режим ініціалізації;

штатний режим роботи.

У режимі ініціалізації TSM забезпечує реєстрацію першого Адміністратора TSM, після чого автоматично переводиться в штатний режим роботи.

60 У штатному режимі роботи TSM забезпечує виконання функцій і дій, що відповідають правам ролі авторизованого користувача.

Зберігання інформації про користувачів.

TSM забезпечує зберігання інформації про користувачів незалежно від їхньої ролі (Користувач або Адміністратор).

Інформація про користувача може містити, наприклад, наступні дані:

- 5 Роль;
- Ім'я;
- Опис;
- Ідентифікатор;
- Додатковий аутентифікатор;
- 10 Дата й час реєстрації;
- Стан блокування (завжди відключено для Адміністратора);
- Загальна кількість входів;
- Кількість послідовних невдалих спроб аутентифікації;
- Дата й час останнього входу;
- 15 Режим контролю цілісності (М'який/Твердий, для Адміністратора завжди М'який).
- Реєстрація подій TSM.

Журнал TSM містить інформацію про події, викликані діями користувачів TSM, а так само про помилки, що відбулися.

Максимальна кількість записів у журналі подій вибирається виходячи з обсягу відведеної під цей журнал пам'яті.

У випадку виявлення несанкціонованої модифікації записів журналу доступ до комп'ютера блокується для всіх користувачів, крім Адміністратора.

При переповненні журналу подій дані про нові події записуються поверх самих старих записів для виключення переповнення журналу.

- 25 Передбачено функцію вивантаження Адміністратором журналу подій з TSM за допомогою додатка для операційних систем, наприклад, таких як: Microsoft Windows XP/2003/Vista/2008/7/2008R2 (x86/x64), Linux (LSB 3.6, 4.0).

В TSM передбачена функція відправлення записів журналу подій TSM на сервер в автоматичному режимі після завантаження операційної системи.

- 30 Висновок зведеної інформації про TSM.

TSM по запиту Адміністратора надає у вигляді звіту, наприклад, наступну інформацію:

- серійний номер екземпляра TSM;
- версія програмного забезпечення TSM;
- модель материнської плати;
- 35 версія BIOS материнської плати;
- список користувачів TSM, відсортований по даті й часу реєстрації користувача, що включає, наприклад, наступну інформацію:

- роль,
- ім'я,
- 40 опис,
- ідентифікатор,
- дата й час реєстрації,
- стан блокування,
- загальна кількість входів,
- 45 кількість послідовних неуспішних спроб аутентифікації,
- дата й час останнього входу,
- режим КЦ;
- інформацію про журнал реєстрації подій, що включає:
- загальну кількість записів у журналі подій,
- 50 кількість записів, що є інформацією про помилки:
- кількість записів, що є подіями зміни інформації про користувачів; інформацію про КЦ, що включає:
- стан активності,
- кількість контрольованих об'єктів ФС;
- 55 можливість використання пароля ІУ за замовчуванням.

Передбачено функцію вивантаження даного звіту за допомогою додатка для операційних систем, наприклад, таких як: Microsoft Windows XP/2003/Vista/2008/7/2008R2 (x86/x64), Linux (LSB 3.6, 4.0).

Контроль цілісності програмного середовища (КЦ).

- 60 Підсистема КЦ забезпечує контроль цілісності для наступних об'єктів:

1. Файли на комп'ютері для файлових систем, наприклад, таких як: NTFS/FAT32/FAT16/Ext2/Ext3;

2. Критичні сектори жорстких дисків:

Master Boot Record;

5 62 сектора після Master Boot Record;

Volume (Partition) Boot Sector для кожного розділу жорсткого диска;

Extended Boot Record для кожного розділу жорсткого диска.

Обчислення контрольних сум об'єктів КЦ виконується по алгоритму MD5.

Контроль цілісності виконується після аутентифікації Користувача або Адміністратора в

10 TSM. До закінчення перевірки КЦ подальше завантаження комп'ютера неможливе.

Передбачено два режими КЦ для користувачів TSM:

1. Твердий (при використанні даного режиму у випадку порушення КЦ подальше завантаження комп'ютера неможливе);

15 2. М'який (при використанні даного режиму у випадку порушення КЦ користувачеві виводиться попередження про порушення КЦ, але подальше завантаження комп'ютера можливе).

Для Адміністраторів завжди активний "М'який" режим КЦ.

Ініціалізація підсистеми КЦ.

20 Процес ініціалізації КЦ являє собою процес формування й збереження списку об'єктів, що підлягають контролю підсистемою КЦ.

За формування списку об'єктів файлової системи (ФС) відповідає додаток для операційних систем, наприклад, таких як: Microsoft Windows XP/2003/Vista/2008/7/2008R2 (x86/x64), Linux (LSB 3.4, 4.0), що виконує наступні функції:

1. Формування списку файлів для КЦ;

25 2. Обчислення контрольних сум для файлів і секторів HDD, що підлягають КЦ;

3. Формування об'єкта (файлу), що містить список об'єктів контролю й контрольні суми.

Додаток виконується у вигляді майстра.

30 Використовувані в цій заявці терміни "засіб", "компонент" і "система" належать до комп'ютерної суті, що являє собою або устаткування, або комбінацію устаткування й програмного забезпечення, або програмне забезпечення, або виконуване програмне забезпечення. Наприклад, компонент може являти собою, але не обмежуючись, спосіб, що виконується на процесорі, процесор, привід жорсткого диска, множинні приводи (оптичного й/або магнітного носія), об'єкт, здійснений модуль, потік виконання, програму й/або комп'ютер.

35 У загальному випадку, програмні модулі містять у собі процедури, програми, об'єкти, компоненти, структури даних і т.д., які виконують певні завдання або реалізують певні абстрактні типи даних. Крім того, фахівцям у даній області техніки очевидно, що способи, що відповідають технічному рішенню, можна здійснювати на практиці за допомогою інших конфігурацій комп'ютерної системи, у тому числі однопроцесорних або багатопроцесорних комп'ютерних систем, міні-комп'ютерів, універсальних комп'ютерів, а також персональних комп'ютерів, кишенькових обчислювальних пристроїв, мікропроцесорних або програмувальних споживчих електронних приладів та ін., кожний їх яких може в ході роботи підключатися до

40 одному або декількох відповідним пристроям.

Комп'ютер звичайно містить у собі різні комп'ютерно-зчитувальні середовища. Комп'ютерно-Зчитувальні середовища можуть являти собою будь-які наявні середовища, до яких комп'ютер може здійснювати доступ, і містять у собі енергозалежні й енергонезалежні середовища, змінні ГІ стаціонарні середовища. У порядку прикладу, але не обмеження, комп'ютерно-зчитувальні середовища можуть містити комп'ютерні носії даних і середовища передачі даних. Комп'ютерні носії даних містять у собі енергозалежні й енергонезалежні, змінні й стаціонарні носії, реалізовані за допомогою будь-якого методу або технології для зберігання інформації, наприклад комп'ютерно-зчитувальних команд, структур даних, програмних модулів або інших даних. Комп'ютерні носії даних містять у собі, але не обмежуючись, RAM, ROM, EEPROM, флеш-пам'ять або іншу технологію пам'яті, CD-ROM, цифрові універсальні диски (DVD) або інші оптичні диски, магнітні касети, магнітну стрічку, накопичувач на магнітних дисках або інші магнітні запам'ятовувальні пристрої або будь-який інший носій, якому можна використовувати

55 для зберігання корисної інформації, і до якого комп'ютер може здійснювати доступ.

Ілюстративна обчислювальна система для реалізації різних аспектів містить у собі комп'ютер, причому комп'ютер містить у собі процесор, системну пам'ять і системну шину. Системна шина забезпечує інтерфейс для системних компонентів, у тому числі, але не обмежуючись, системної пам'яті до процесора. Процесор може являти собою кожний з різних

комерційно доступних процесорів. Як процесор також можна застосовувати подвійні мікропроцесори й інші багатопроцесорні архітектури.

Системна шина може являти собою кожну з декількох типів шинних структур, і може додатково підключатися до шини пам'яті (за допомогою контролера пам'яті або без нього), периферійній шині й локальній шині з використанням будь-яких різноманітних комерційно доступних шинних архітектур. Системна пам'ять містить у собі постійну пам'ять (ROM) і оперативну пам'ять (RAM). BIOS зберігається в енергонезалежній пам'яті, наприклад, ROM, EEROM, EEPROM, причому BIOS містить основні процедури, які допомагають переносити інформацію між елементами комп'ютера, наприклад, при запуску. RAM також може містити в собі високошвидкісне RAM, наприклад, статичне RAM для кешування даних.

Комп'ютер додатково містить у собі внутрішній привід жорсткого диска (HDD) (наприклад, EIDE, SATA), причому внутрішній привід жорсткого диска також можна пристосувати для зовнішнього використання в підходящому корпусі (не показаний), привід магнітного флопі-диска (FDD), (наприклад, для читання з або запису на змінну дискету) і привід оптичного диска, (наприклад, що читає диск CD-ROM або для читання з або запису на інші оптичні носії високої ємності, наприклад, DVD). Привід жорсткого диска, привід магнітного диска й привід оптичного диска можуть бути підключені до системної шини за допомогою інтерфейсу приводу жорсткого диска, інтерфейсу приводу магнітного диска й інтерфейсу оптичного приводу, відповідно. Інтерфейс для реалізації зовнішнього приводу містить у собі щонайменше одну або обидві з технологій універсальної послідовної шини (USB) і інтерфейсу IEEE 1394.

Приводи й відповідні комп'ютерні носії даних забезпечують енергонезалежне сховище даних, структур даних, комп'ютерних інструкцій і т.д. Для комп'ютера, приводи й носії забезпечують зберігання будь-яких даних у підходящому цифровому форматі. Хоча вищенаведений опис комп'ютерно-зчитувальних носіїв належить до HDD, змінній магнітній дискеті й змінним оптичним носіям, наприклад, CD або DVD, фахівцям у даній області техніки очевидно, що інші типи носіїв, які зчитуються комп'ютером, наприклад, зір-диски, магнітні касети, карти флеш-пам'яті, картриджі, і т.п., також моно використовувати в ілюстративному операційному середовищі, і, крім того, що будь-які такі носії можуть містити комп'ютерні інструкції для здійснення нових способів розкритої архітектури.

На приводах і RAM може зберігатися ряд програмних модулів, у тому числі операційна система, одна або декілька прикладних програм, інші програмні модулі й програмні дані. Повністю або частково, операційна система, додатки, модулі й/або дані також можуть кешуватися в RAM. Також очевидно, що розкриту архітектуру також можна реалізувати з різними комерційно доступними операційними системами або комбінаціями операційних систем.

Користувач може вводити команди й інформацію в комп'ютер через один або декілька дрових/бездротових пристроїв введення, наприклад клавіатуру й вказівний пристрій, наприклад, миша. Пристрої введення/виведення можуть містити в собі мікрофон/гучномовці й інший пристрій, наприклад ІК пульт керування, джойстик, ігрова панель, перо, сенсорний екран та ін. Ці й інші пристрої введення нерідко підключені до процесора через інтерфейс пристроїв введення, що підключений до системної шини, але можуть підключатися за допомогою інших інтерфейсів, наприклад, паралельного порту, послідовного порту IEEE 1394, ігрового порту, порту USB, ІК інтерфейсу й т.д.

Монітор або пристрій відображення іншого типу також підключений до системної шини через інтерфейс, наприклад, відеоадаптер. Крім монітора, комп'ютер звичайно містить у собі інші периферійні пристрої виведення, наприклад гучномовці, принтери й т.д.

Вище були описані приклади розкритої архітектури. Звичайно, неможливо описати всі мислимі комбінації компонентів або способів, але фахівцям в даній області техніки очевидно, що можливо багато додаткових комбінацій і перестановки. Відповідно, нова архітектура покликана охоплювати всі такі зміни, модифікації й варіації, які відповідають суті й обсягу формули корисної моделі. Крім того, у тому ступені, у якому термін "містить у собі" використовується в докладному описі або у формулі винаходу, такий термін покликаний бути включаючим аналогічно терміну "утримуючий", оскільки "утримуючий" інтерпретується при використанні як перехідне слово у формулі.



## ФОРМУЛА КОРИСНОЇ МОДЕЛІ

1. ПЕОМ із захистом від несанкціонованого доступу (НСД), що містить системну шину, базову систему введення/виведення (BIOS) і модуль безпеки TSM, що вбудовується, підключений до BIOS, причому BIOS виконано з можливістю передавати керування завантаженням ПЕОМ TSM після проходження процедури Power On Self-Test (POST), при цьому TSM містить засіб для блокування доступу до налаштувань BIOS усім, крім авторизованих адміністраторів TSM, засіб для аутентифікації користувача/адміністратора TSM, причому аутентифікація користувача/адміністратора виконується за допомогою ідентифікуючого пристрою (ІУ), що підключається до системної шини ПЕОМ, засіб для передачі керування BIOS для подальшого завантаження комп'ютера після аутентифікації користувача/адміністратора.
2. ПЕОМ із захистом від НСД за п. 1, який **відрізняється** тим, що TSM додатково містить блок пам'яті для зберігання журналу TSM, що містить інформацію про події, викликані діями користувачів TSM, а також про помилки, що відбулися.
3. ПЕОМ із захистом від НСД за п. 2, який **відрізняється** тим, що TSM додатково містить засіб для виявлення несанкціонованої модифікації записів журналу.
4. ПЕОМ із захистом від НСД за п. 3, який **відрізняється** тим, що TSM додатково містить засіб блокування доступу до ПЕОМ для всіх, крім адміністратора, у випадку виявлення несанкціонованої модифікації записів журналу.
5. ПЕОМ із захистом від НСД за п. 4, який **відрізняється** тим, що містить засіб контролю цілісності (КЦ) програмного середовища ПЕОМ та засіб для передачі керування BIOS для подальшого завантаження комп'ютера після контролю цілісності.
6. ПЕОМ із захистом від НСД за п. 5, який **відрізняється** тим, що контроль цілісності виконують за допомогою порівняння контрольних сум об'єктів КЦ, причому обчислення контрольних сум об'єктів КЦ виробляється по алгоритму MD5.



Фиг. 1

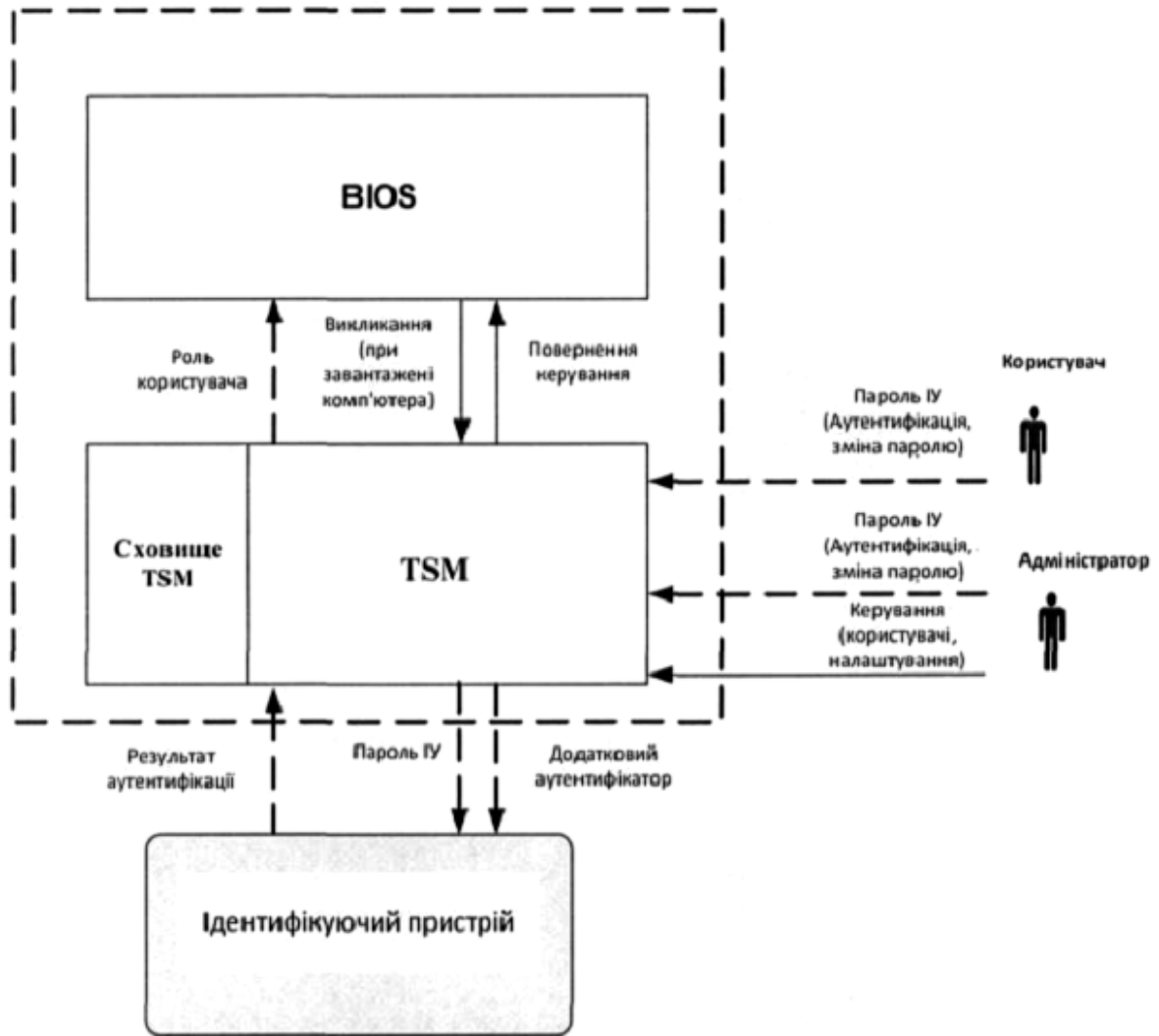


Fig. 2