



УКРАЇНА

(19) UA

(11) 44303

(13) C2

(51) 6 G06F12/14

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ НА ВИНАХІД

(54) ПОРТАТИВНА ЧІП-КАРТКА

1

2

(21) 97094557

(22) 07 03 1996

(24) 15 02 2002

(86) PCT/DE96/00407, 07 03 1996

(31) 195 08 723 2

(32) 10 03 1995

(33) DE

(46) 15 02 2002, Бюл. № 2, 2002 р.

(72) Вайнлендер Маркус, DE

(73) СІМЕНС АКЦІОНГЕЗЕЛЬШАФТ, DE

(56) EP 0449255 A, 02 10 91

DE 4115152 A, 12 11 92

(57) 1 Портативна чіп-картка, що містить процесор та запам'ятовуючий пристрій, пам'ять якого розділена на область пам'яті операційної системи та принаймні одну область пам'яті користувача, яка відрізняється тим, що процесор стосовно внутрішніх мікрокодів настроєний таким чином, що блоковано виконання завантажених в область пам'яті користувача стандартних команд процесора, що вимагають доступу до комірок пам'яті з метою зчитування або запису, в області пам'яті операційної системи передбачена таблиця доступу до областей пам'яті, яка для кожної області пам'яті користувача має доступні області адрес для стандартних команд процесора, завантажених в область пам'яті користувача, процесор виконаний з можливістю за допомогою передбаченої у його операційній системі програми, яка викликається завантаженою в область пам'яті користувача стандартною командою процесора, що вимагає доступу до комірок пам'яті з метою зчитування або запису, перевіряти з використанням таблиці доступу до областей пам'яті, чи знаходиться передба-

чене даною стандартною командою процесора звертання до комірки пам'яті в дозволеній області адрес, і якщо ні - блокувати виконання стандартної команди процесора

2 Портативна чіп-картка за п. 1, яка відрізняється тим, що процесор стосовно внутрішніх мікрокодів настроєний з можливістю перед виконанням стандартних команд процесора, що вимагають доступу до комірок пам'яті з метою зчитування або запису, перевіряти поточний вміст програмного лічильника процесора, що відповідає певній стандартній команді процесора, у разі, коли вміст програмного лічильника вказує на адресу комірки пам'яті, що лежить в області пам'яті операційної системи, виконання стандартної команди дозволяється, у разі, коли вміст програмного лічильника вказує на адресу комірки пам'яті, що лежить в області пам'яті користувача, виконання стандартної команди процесора блокується

3 Портативна чіп-картка за п. 1 або п. 2, яка відрізняється тим, що процесор виконаний з можливістю за допомогою передбаченої його операційною системою програми перевіряти поточний вміст стека процесора, який відповідає стандартній команді процесора, що вимагає доступу до комірок пам'яті з метою зчитування або запису, порівнювати запис у таблиці доступу до областей пам'яті, який відповідає згаданому вмісту стека, з передбаченим стандартною командою процесора доступом до комірки пам'яті і блокувати виконання стандартної команди процесора у разі, коли згаданий доступ вказує на комірку пам'яті, що лежить поза вказаною в таблиці доступу до областей пам'яті, доступною областю

Винахід стосується системи обробки даних із захистом пам'яті для багатьох користувачів, зокрема портативної чіп-картки

Пристрій обробки даних за всіма правилами як суттєві робочі засоби містить процесор та запам'ятовуючий пристрій (ЗП). В ЗП, по-перше, записуються оброблювані процесором команди, а по-друге — процесор може записувати результати обробки. Зазвичай вся наявна в розпорядженні,

тобто адресована процесором, пам'ять розділена принаймні на дві окремі області. В першу область, яка в подальшому буде називатись областю пам'яті операційної системи, при виготовленні пристрою обробки даних заносяться так звані коди операційної системи, за допомогою яких зокрема здійснюється керування апаратними компонентами системи

В другу область, яка в подальшому буде нази-

(13) C2

(11) 44303

(19) UA

ватись областю пам'яті користувача, можуть бути записані програми та дані, підготовлені самим користувачем пристроєм обробки даних

З точки зору процесора пристроєм обробки даних, між цими областями пам'яті не існує різниці. Зокрема, не має ніякого значення, чи розділена фізично загальна область адрес мікропроцесора – як це має місце в портативних пристроях обробки даних, таких як процесорні чіп-картки, – на незмінну пам'ять (наприклад, постійний запам'ятовуючий пристрій, ПЗП) та енергонезалежну пам'ять користувача (наприклад, програмований постійний запам'ятовуючий пристрій з електричним стиранням, ЕППЗП). Процесор, використовуючи всю область адрес, звертається при необхідності до будь-якого запам'ятовуючого елемента, незалежно від того, знаходиться він в області пам'яті операційної системи, чи в області пам'яті користувача. Однак, наслідком цього є те, що за допомогою індивідуального програмного коду, тобто командами користувача, записаними користувачем в зарезервовану для нього область пам'яті портативного пристрою обробки даних, необережним або навмисним чином може бути безперешкодно одержаний доступ для зчитування та/або зміни як вмісту області пам'яті операційної системи, так і вмісту областей, виділених для інших користувачів, та інсталюваних там програм або даних користувачів.

В європейському патенті EP 05 61 509 A1 описана розгалужена комп'ютерна система з великою кількістю терміналів користувачів, а також інтерфейсами введення та виведення. Управління комп'ютерною системою здійснюється операційною системою, наприклад UNIX. Наперед визначені команди операційної системи або інтерфейси введення та виведення в комп'ютерній системі для користувачів в загальному випадку можуть бути заблокованими. Під контролем операційної системи вони можуть бути опосередковано викликані чи активізовані шляхом введення користувачем додаткових команд операційної системи, якщо він має записаний в пам'яті дозвіл на доступ.

В патенті FPH DE 41 15 152 A1 описана мікропроцесорна система із захистом даних для портативних носіїв даних. Вона містить відокремлену від вмонтованої мікропроцесорної схеми додаткову схему захисту, яка забезпечує "чужий" програмний доступ лише до тих областей пам'яті, до яких у неї є дозвіл. При цьому в першому варіанті реалізації додаткова схема захисту містить перший компаратор з допоміжним регістром і другий компаратор з допоміжним регістром. Присвоєні користувачеві граничні значення для доступу до областей пам'яті записані або в провідниковому ПЗП, або в надійному ЗП і завантажуються вмонтованим мікропроцесором в допоміжні регістри. За допомогою компараторів їх вміст порівнюється з адресним регістром та програмним лічильником вмонтованої мікропроцесорної схеми. Вихідні значення компараторів об'єднуються логічним елементом AND і подаються на схему управління вмонтованої мікропроцесорної системи. У другому варіанті реалізації додаткова схема захисту містить власний процесор захисту зі схемою ділення тактової частоти та власним запам'ятовуючим пристроєм. У цьому варіанті реалізації присвоєні користувачеві

граничні значення для доступу до областей пам'яті запам'ятовуються і порівнюються процесором захисту з вмістом адресного регістра та програмного лічильника мікропроцесорної схеми.

В основу винаходу покладено задачу розробки захисту доступу до пам'яті для портативних чіп-карток, який обходився б без втручання в апаратну структуру чіп-картки.

Поставлена задача розв'язана тим, що спочатку процесор, зокрема стосовно внутрішніх кодів, настроєний таким чином, що блоковано виконання записаних в області пам'яті користувачів стандартних команд процесора, які потребують доступу для зчитування або зміни вмісту комірок пам'яті. Крім того, в області пам'яті операційної системи є таблиця доступу до областей пам'яті, яка для кожної області пам'яті користувача має доступні області адрес для команд, завантажених в кожну область пам'яті користувача. Нарешті, процесор виконаний з можливістю за допомогою передбаченої у його операційній системі програми, яка викликається стандартною командою процесора, завантаженою в області пам'яті користувача, що вимагає доступу до комірок пам'яті для здійснення зчитування чи запису, і перевіряти з використанням таблиці доступу до областей пам'яті, чи знаходиться в дозволений області адрес звертання до комірки пам'яті, яке передбачене даною стандартною командою, і якщо ні – блокувати виконання стандартної команди процесора.

Перевагою винаходу є те, що "радіус дії" однієї або кількох наявних в області пам'яті програм користувачів може бути простим чином обмежений визначеною областю пам'яті пристроєм обробки даних, лише програмно-технічними засобами, без додаткових апаратних засобів. Область адрес пам'яті, дозволена для зчитування та запису командами програми користувача, для кожного користувача може бути записана в таблиці доступу до областей пам'яті. Як правило, дозволена область адрес співпадає з наданою в розпорядження користувача областю пам'яті, що містить індивідуальні коди програм користувача. Таким чином, користувачеві заборонено за допомогою його програмних кодів здійснювати доступ для запису та зчитування із наданої йому області пам'яті до комірок пам'яті, що лежать або в області пам'яті, наданій іншому користувачеві, або в області пам'яті операційної системи.

Нижче винахід пояснюється з використанням прикладу, зображеного на фігурі. Вона відображає типовий розподіл пам'яті пристроєм обробки даних, який називають також розбивкою пам'яті. При цьому вся пам'ять розділена на дві частини. Верхня, так звана область пам'яті операційної системи, область адрес якої починається зі стартової адреси 0000h (h = шістнадцяткове кодування), слугує для приймання кодів операційної системи. Операційна система організує в основному управління процесора, роботу можливо наявних інших робочих засобів пристрою обробки даних, а також доступ до пам'яті. До неї примикає область пам'яті користувачів, область адрес якої в зображеному прикладі починається зі стартової адреси 8000h (h = шістнадцяткове кодування), і яка слугує для приймання програм та даних як правило різних корис-

тувачів. Ця область, таким чином, пам'яті розподілена на підобласті. В наведеному на фігурі прикладі зображено дві такі підобласті. Одна підобласть, що охоплює адреси від 8000h до 8FFFh, відведена користувачеві А для запису його програм та даних. До неї примикає підобласть, що охоплює адреси від 9000h до 9FFFh і також відведена користувачеві В для його програм та даних. Від наступної стартової адреси A000h до кінця об'єму запам'ятовуючого пристрою з адресою FFFFh можуть бути розташовані підобласті інших користувачів.

Таким чином, в зображеному прикладі, наприклад, користувач А, якому відведена область пам'яті в області адрес від 8000h до 8FFFh, на основі інстальованих в ній програмних кодів користувача може одержати доступ лише до даних користувача, коди яких також лежать в комітках пам'яті, адресний простір котрих сягає від початкової адреси 8000h до кінцевої адреси 8FFFh. Згідно з винаходом, це забезпечується шляхом відповідного запису в комірку області пам'яті операційної системи, позначений в таблиці доступу міткою "Програма користувача А". В представленому на фігурі прикладі це відображено допустимим розгалуженням програми користувача А в межах власної області пам'яті для програм, показаних спрямованою вперед, позначеною індексом S1, суцільною лінією. Всі інші програмні розгалуження, що виходять із цієї області пам'яті для програм користувача, такі як спрямоване в область пам'яті операційної системи розгалуження S5 або розгалуження S3, спрямоване в область пам'яті користувача, сусідню з областю пам'яті користувача А, є недопустимими і, таким чином, виконуватись не будуть. Такі розгалуження на фігурі зображені пунктирними лініями.

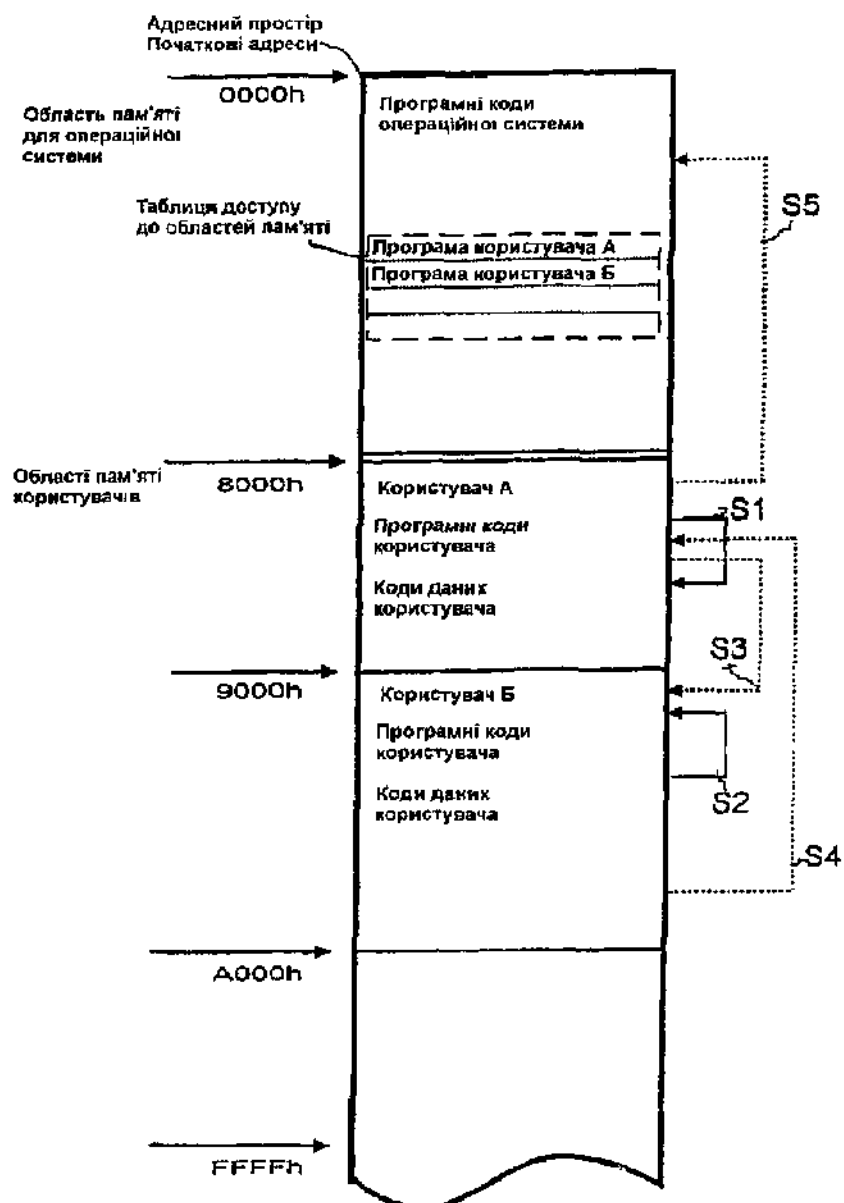
Таким же чином для іншого користувача В, що інстальював свої програмні коди в діапазоні адрес області пам'яті від 9000h до 9FFFh, для програмних кодів можливий доступ для зчитування та запису даних лише в межах власної області пам'яті, наприклад, для спрямованого назад програмного розгалуження S2. Зображене на" фігурі пунктирною лінією S4 звертання, що виходить від цієї області пам'яті для програм користувача і спрямоване на область пам'яті користувача А, також є недопустимим і згідно з винаходом може бути забороненим.

Настроюку процесора стосовно його внутрішніх мікрокодів здійснено таким чином, що перед

виконанням стандартних команд процесора, що вимагають доступу до вмісту комірок пам'яті з метою зчитування або запису, спочатку перевіряється відповідний даний стандартній команді вміст програмного лічильника процесора. Лічильник "вказує" на походження команди, що в даний момент підлягає виконанню. В разі, коли вміст програмного лічильника вказує на адресу комірки пам'яті, що лежить в області пам'яті операційної системи, тобто команда є складовою операційної системи, дається дозвіл на виконання команди. В даному разі походження команди зумовлене не користувачем, а системою. І навпаки, коли вміст програмного лічильника вказує на адресу комірки пам'яті, що лежить в області пам'яті користувача, виконання команди блокується. В цьому разі джерело команди однозначно зумовлене користувачем.

Згідно з винаходом, виконання таких команд можливе обхідним шляхом через програму, що є в операційній системі процесора. Ця програма організована таким чином, що спочатку перевіряється відповідний команді звертання до комірки пам'яті поточний вміст стека процесора. В цьому стеку міститься адреса повернення команди, яка також відображає "походження" команди, що підлягає виконанню. Потім – запис в таблиці доступу до областей пам'яті, відповідний вмісту стека, порівнюється із передбаченим командою доступом до комірки пам'яті. У разі, коли передбачений доступ вказує на комірку пам'яті, що лежить поза вказаним в таблиці доступу до областей пам'яті доступною областю адрес, виконання команди блокується, в іншому разі дозволяється.

Пристрій обробки даних згідно з винаходом особливо придатний для мобільного використання, оскільки саме тут потрібне багаторазове паралельне використання кількох користувачами. При цьому кожен користувач може використовувати пристрій обробки даних без побоювання завдання шкоди його даним іншими користувачами і без випадкового ушкодження програм та даних інших користувачів. Зокрема забезпечено захист даних користувачів один від одного, а також заборонене неправомірне або непрофесійне звертання з метою зчитування та запису до операційної системи з боку програмних кодів користувачів, інстальованих в області пам'яті для програм користувачів. Мобільними пристроями обробки даних, згідно з винаходом, можуть бути зокрема процесорні чіп-картки.



Фіг.