РЕСПУБЛИКА КАЗАХСТАН

(19) **KZ** (13) **U** (11) **3644**
(51) ***G06F 12/14*** (2006.01)
G06F 21/00 (2006.01)

МИНИСТЕРСТВО ЮСТИЦИИ РЕСПУБЛИКИ КАЗАХСТАН

ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ
К ПАТЕНТУ

(21) 2018/0765.2
(22) 23.10.2018
(45) 08.02.2019, бюл. №6
(72) Иманов Талгат Сундеткалиевич; Сейлова Нургуль Абадуллаевна; Ананич Геннадий Михайлович; Кабенко Романа Витальевич; Жұмағали Сабыржан Жанбулатұлы; Қажымұқан Қамбар Саматұлы; Иманбаев Азамат Жанатұлы; Богуспаев Нурлан Болаткаримович; Лебедев Кирилл Александрович; Таласбеков Жанибек Асылбекович
(73) Некоммерческое акционерное общество "Казахский национальный исследовательский технический университет имени К.И. Сатпаева"
(56) KZ 12969, 15.04.2003

(54) **СПОСОБ ЗАЩИТЫ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА**

(57) Полезная модель относится к области вычислительной техники, в частности к области обеспечения безопасности информации и может быть использована для защиты персонального компьютера от несанкционированного доступа к информации, хранимой в персональных компьютерах.

Технический результат достигается способом защиты персонального компьютера от несанкционированного доступа, заключающийся в том, что с помощью электронного средства проверяется разрешение доступа к информации, хранящейся на ПЭВМ, по результатам которого производится активация или блокировка цепи питания ПЭВМ. Согласно полезной модели в качестве электронного средства используют устройство защиты от несанкционированного доступа к информации с энергонезависимой памятью, содержащего устройство идентификации, коммуникационную плату и программное обеспечение. В коммуникационной плате создают базу с идентификационными данными пользователей, при обращении к ПЭВМ пользователей коммуникационная плата производит их регистрацию, идентификацию и аутентификацию путем сравнения, хранящихся в ней данных с входными данными с устройства идентификации, после обработки информации о пользователях коммуникационная плата подает сигнал активировать или блокировать цепь питания ПЭВМ.

(19) KZ (13) U (11) 3644

Полезная модель относится к области вычислительной техники, в частности к области обеспечения безопасности информации и может быть использована для защиты персонального компьютера от несанкционированного доступа к информации, хранимой в персональных компьютерах.

Известно устройство защиты информации, хранящейся в персональном компьютере (патент РФ №2099779, бюл. №35, опубл. 20.12.97), содержащее внешний носитель информации, выполненный в виде энергонезависимой памяти, и расположенные на общей плате микропроцессор, к которому подключены интерфейс обмена информацией с внешним носителем информации. Устройство также содержит оперативное запоминающее устройство и интерфейс обмена информацией с персональной электронно-вычислительной машиной (далее - ПЭВМ), соединенный с оперативным запоминающим устройством, физический датчик случайных чисел и постоянное запоминающее устройство, предназначенное для хранения программ защиты информации, предотвращения несанкционированного доступа к персональной ПЭВМ, открытого распределения ключей и цифровой подписи.

Недостатками известного устройства являются ограниченные функциональные возможности, заключающиеся в фиксированном интерфейсе обмена информацией с внешним устройством, низкой стойкости к несанкционированным доступам и как следствие возможности несанкционированного считывания данных из внешнего носителя информации.

Известно устройство защиты от несанкционированного доступа к информации (патент РФ №2402810, бюл. №30. опубл. 27.10.2012), содержащее микропроцессор, первая группа входов-выходов которого соединена с группой входов-выходов оперативного запоминающего устройства, постоянное запоминающее устройство, внешний носитель информации, выполненный в виде энергонезависимой памяти, вход-выход которого соединен с первым входом-выходом интерфейса обмена информацией с внешним носителем информации. Известное устройство также содержит устройство индикации, устройство управления индикацией, устройство ввода, устройство управления вводом, репрограммируемое постоянное запоминающее устройство, устройство управления репрограммируемым постоянным запоминающим устройством, первый и второй интерфейсы обмена информацией с внешними устройствами и коммутатор интерфейсов.

Недостатками известного устройства являются избыточность составных блоков, низкая стойкость к несанкционированным доступам вследствие возможности несанкционированного доступа к информации, хранящейся в перепрограммируемом постоянном запоминающем устройстве.

Наиболее близким аналогом к заявляемому способу является способ защиты данных в персональной ЭВМ заключающийся в том, что с помощью электронного средства проверяют разрешение доступа к защищаемой области на физическом носителе информации ЭВМ и разрешение проводить операции с информацией, находящейся на данной области, по результатам которого производится активация или блокировка цепи питания персонального компьютера. (KZ 12969, бюл. №4 от 15.04.2003)

Однако данное устройство не может предотвратить несанкционированный доступ к ресурсам пользователей и требует дополнительных организационно-технических мер для хранения и верификации находящейся в персональном компьютере информации.

Задачей полезной модели является разработка способа защиты персонального компьютера от несанкционированного доступа, позволяющего повысить эффективность защиты информации, хранящейся на ПЭВМ от несанкционированного доступа, а также уменшить себестоимость без снижения функциональных возможностей.

Технический результат, на достижение которого направлено заявляемая полезная модель, заключается в повышении стойкости к несанкционированным доступам к информации, хранящейся на ПЭВМ.

Технический результат достигается способом защиты персонального компьютера от несанкционированного доступа, заключающийся в том, что с помощью электронного средства проверяется разрешение доступа к информации, хранящейся на ПЭВМ, по результатам которого производится активация или блокировка цепи питания ПЭВМ. Согласно полезной модели в качестве электронного средства используют устройство защиты от несанкционированного доступа к информации с энергонезависимой памятью, содержащего устройство идентификации, коммуникационную плату и программное обеспечение. В коммуникационной плате создают базу с идентификационными данными пользователей, при обращении к ПЭВМ пользователей коммуникационная плата производит их регистрацию, идентификацию и аутентификацию путем сравнения, хранящихся в ней данных с входными данными с устройства идентификации, после обработки информации о пользователях коммуникационная плата подает сигнал активировать или блокировать цепь питания ПЭВМ.

Способ защиты персонального компьютера от несанкционированного доступа осуществляется с использованием устройства защиты от несанкционированного доступа к информации (далее - УЗ НСД).

УЗ НСД 1 предназначено для считывания индивидуальных идентификаторов пользователей, с целью их идентификации, аутентификации, регистрации и выполнено в виде микроконтроллера с энергонезависимой памятью, которое может получать питание от ПЭВМ или от автономного аккумулятора. Данное устройство содержит коммуникационную плату (КП) 2 и устройство

идентификации и аутентификации (УИ) 3, которые работают под управлением оригинального программного обеспечения (ПО). Программное обеспечение хранится в программируемом постоянном запоминающем устройстве на самом УЗ НСД 1.

В КП 2 создают базу с идентификационными данными пользователей. КП 2 осуществляет обмен данными с УИ 3, а также регистрацию, идентификацию индивидуальных данных пользователей и связь с интерфейсной программой.

Входные данные пользователей хранятся в УИ 3, которое реализует функцию чтения и первичной обработки идентификационных данных пользователей.

Способ защиты персонального компьютера от несанкционированного доступа поясняется функциональной схемой приведенной на Фигуре и осуществляется следующим образом.

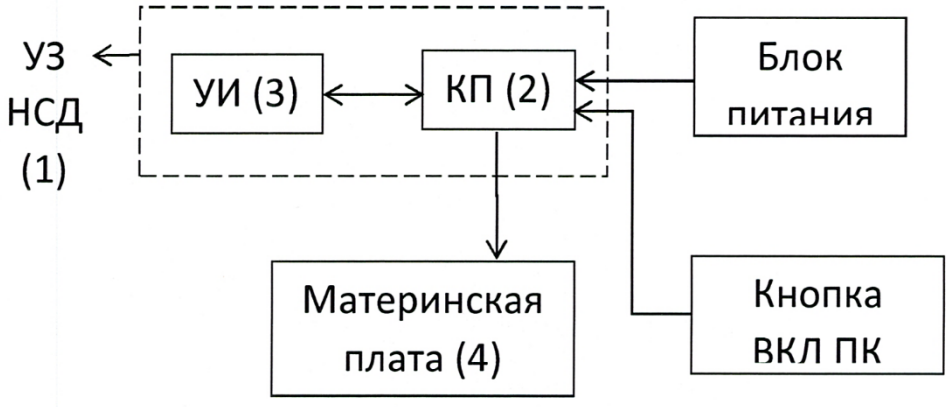
При первом обращении системный администратор настраивает ПЭВМ и УЗ НСД 1. Далее он записывает в УЗ НСД 1 данные пользователей, таким образом, создавая в памяти УЗ НСД 1 базу с идентификационными данными пользователей.

При обращении пользователя с целью его допуска к информации хранящейся на ПЭВМ УЗ НСД производит аутентификацию, идентификацию и регистрацию пользователя. Это происходит путем сравнения записанных и хранящихся данных пользователей в КП 2 с данными на УИ 3, которое работает под управлением КП 2. При несовпадении входных данных с УИ 3 с данными базы идентификационных данных пользователей на КП 2, последний блокирует цепь питания ПЭВМ, а информация о несанкционированных попытках входа регистрируется в КП 2.

Таким образом, способ защиты персонального компьютера от несанкционированного доступа позволяет повысить эффективность защиты информации, хранящейся на ПЭВМ от несанкционированного доступа и позволяет реализовать механизм регистрации попыток не санкционированного доступа к ПЭВМ не зарегистрированных пользователей.

ФОРМУЛА ПОЛЕЗНОЙ МОДЕЛИ

Способ защиты персонального компьютера от несанкционированного доступа, заключающийся в том, что с помощью электронного средства проверяют разрешение доступа к информации, хранящейся на персональной электронно-вычислительной машине, по результатам которого производит активацию или блокировку цепи питания ПЭВМ, ***отличающийся*** тем, что в качестве электронного средства используют устройство защиты от несанкционированного доступа к информации с энергонезависимой памятью, содержащего устройство идентификации, коммуникационную плату и программное обеспечение, в коммуникационной плате создают базу с идентификационными данными пользователей, при обращении к ПЭВМ пользователей коммуникационная плата производит их регистрацию, идентификацию и аутентификацию путем сравнения, хранящихся в ней данных с входными данными с устройства идентификации, после обработки информации о пользователях коммуникационная плата подает сигнал активировать или блокировать цепь питания ПЭВМ.



Фигура

Верстка З. Абылкасымова
Корректор Б. Омарова