РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 632 122**(13) **C2**

(51) МПК
G06F 21/34 (2013.01)
G06F 21/83 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2015112961, 08.04.2015**

(24) Дата начала отсчета срока действия патента:
08.04.2015

Дата регистрации:
02.10.2017

Приоритет(ы):
(30) Конвенционный приоритет:
09.04.2014 TW 103113026

(43) Дата публикации заявки: **27.10.2016** Бюл. № **30**

(45) Опубликовано: **02.10.2017** Бюл. № **28**

Адрес для переписки:
109012, Москва, ул. Ильинка, 5/2, ООО "Союзпатент"

(72) Автор(ы):
ЧОУ Хун-Чиэнь (TW)

(73) Патентообладатель(и):
ЧОУ Хун-Чиэнь (TW)

(56) Список документов, цитированных в отчете о поиске: **RU 2423734 C2, 10.07.2011. RU 2388051 C2, 27.04.2010. CN 101739527 A, 16.06.2010. WO 2012/026666 A2, 01.03.2012. CN 103200011 A, 10.07.2013. US 2012/0303964 A1, 29.11.2012.**

(54) СПОСОБ И УСТРОЙСТВО ПРОВЕРКИ ПАРОЛЯ ДЛЯ ПРОВЕРКИ ВХОДНОГО ПАРОЛЯ И КОМПЬЮТЕРНАЯ СИСТЕМА, СОДЕРЖАЩАЯ УСТРОЙСТВО ПРОВЕРКИ ПАРОЛЯ

(57) Реферат:

Изобретение относится к компьютерной безопасности. Технический результат заключается в повышении безопасности при проверке вводимого пароля. Способ, осуществляемый устройством проверки пароля, содержит этапы, на которых в ответ на запрос ввода пароля от прикладной управляющей программы формируют и передают к компьютерному модулю данные изображения виртуальной клавиатуры, чтобы отображать на модуле отображения виртуальную клавиатуру, в ответ на операцию виртуальной клавиатуры формируют данные пароля и составляют соответствующий им входной пароль, в ответ на запрос подтверждения пароля от устройства ввода сравнивают входной пароль и заранее установленный пароль; причем данные пароля содержат последовательность местоположений нажатий на виртуальной клавиатуре, и прикладная управляющая программа получает множество наборов координат для местоположений нажатий на виртуальной клавиатуре согласно данным операции и посылает наборы координат на устройство проверки пароля в качестве данных пароля, устройство проверки пароля определяет буквенно-цифровые символы, соответственно отображаемые на виртуальной клавиатуре в местоположениях нажатий в соответствии с наборами координат, когда событие нажатия сохранено в устройстве проверки пароля. 3 н. и 19 з.п. ф-лы, 6 ил.

RU 2632122 C2

RU 2632122 C2

Фиг. 3

RU 2632122 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 632 122**(13) **C2**

(51) Int. Cl.
G06F 21/34 (2013.01)
G06F 21/83 (2013.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2015112961, 08.04.2015**

(24) Effective date for property rights:
08.04.2015

Registration date:
02.10.2017

Priority:
(30) Convention priority:
09.04.2014 TW 103113026

(43) Application published: **27.10.2016** Bull. № **30**

(45) Date of publication: **02.10.2017** Bull. № **28**

Mail address:
109012, Moskva, ul. Ilinka, 5/2, OOO "Soyuzpatent"

(72) Inventor(s):
CHOU Khun-Chien (TW)

(73) Proprietor(s):
CHOU Khun-Chien (TW)

(54) METHOD AND PASSWORD VERIFICATION DEVICE FOR INSPECTING INPUT PASSWORD AND COMPUTER SYSTEM CONTAINING PASSWORD VERIFICATION DEVICE

(57) Abstract:

FIELD: information technology.

SUBSTANCE: method performed by the password verification device includes the steps, which in response to the request password input from application control program is formed and the image data of the virtual keyboard are transmitted to the computer module, to display the virtual keyboard on the module display, in response to the operation of the virtual keyboard the password information and account corresponding to the input password are formed, in response to the confirmation password from the input device the input password and the predetermined password are compared. The password data comprise a sequence of locations of the clicks on the virtual keyboard, and the application control program obtains a plurality of sets of coordinates for the locations of the clicks on the virtual keyboard according to the operation data and sends the coordinate sets to the password verification device as password data, the password verification device determines the alphanumeric characters respectively displayed on the virtual keyboard at the location of the clicks in accordance with the coordinate sets, when the click event is saved in the password verification device.

EFFECT: increasing the security, when verifying the password.

22 cl, 6 dwg

RU 2632122 C2

RU 2632122 C2

Фиг. 3

RU 2632122 C2

Перекрестная ссылка на связанную заявку

Настоящая заявка заявляет приоритет тайваньской заявки №103113026, поданной 9 апреля 2014 г.

Область техники, к которой относится заявка

Раскрытие относится к способу и устройству проверки пароля для проверки введенного пароля и к компьютерной системе, содержащей устройство проверки пароля для реализации способа.

Уровень техники

Публикация №200905541 тайваньского патента раскрывает способ введения ключа, использующий динамическую моделированную клавиатуру. Способ обеспечивает моделированную клавиатуру, выполненную с возможностью динамического изменения позиций ее клавиш. Использование этого способа позволяет избежать кражи такого контента, как введенный пароль, посредством "регистрации клавиш".

Однако, операционная система компьютерного устройства может быть отобрана насильно третьим лицом, позволяя третьему лицу регистрировать деятельность компонент ввода компьютерного устройства (мышь, клавиатура и т.п.) и получать снимок экрана блока отображения, подключенного к компьютерному устройству. Поэтому безопасность введенного контента все еще подвергается риску.

Сущность изобретения

Поэтому задача раскрытия заключается в обеспечении способа, который может смягчить по меньшей мере один из недостатков предшествующего уровня техники.

В соответствии с раскрытием, способ проверки введенного пароля должен реализовываться устройством проверки пароля. Устройство проверки пароля электрически подключается между устройством ввода и электронным устройством. Электронное устройство содержит компьютерный модуль, исполняющий операционную систему (OS), установленную с прикладной управляющей программой, и модуль отображения, электрически соединенный с компьютерным модулем. Устройство проверки пароля является независимым автономным устройством и хранит заранее установленный пароль. Способ содержит этапы, на которых:

в ответ на запрос ввода пароля от прикладной управляющей программы формируют данные изображения, связанные с виртуальной клавиатурой, и передают данные изображения на компьютерный модуль, так что компьютерный модуль управляет модулем отображения для отображения на нем виртуальной клавиатуры;

в ответ на данные пароля, связанные с работой виртуальной клавиатуры от прикладной управляющей программы, составляют входной пароль, соответствующий данным пароля; и

в ответ на запрос подтверждения пароля от устройства ввода, сравнивают введенный пароль и заранее установленный пароль.

Другая задача раскрытия заключается в обеспечении устройства проверки пароля, выполненного с возможностью реализации вышеупомянутого способа.

В соответствии с раскрытием, устройство проверки пароля является независимым автономным устройством и электрически подключается между устройством ввода и электронным устройством. Устройство проверки пароля содержит блок формирования виртуальных клавиш, блок запоминающего устройства, процессорный блок и блок сравнения.

Блок формирования виртуальных клавиш выполнен с возможностью формирования, в ответ на запрос ввода пароля от электронного устройства, данных изображения, связанных с виртуальной клавиатурой, и передачи данных изображения электронному

устройству. Заранее установленный пароль сохраняется в блоке запоминающего устройства.

Процессорный блок выполнен с возможностью составления входного пароля, соответствующего данным пароля, в ответ на данные пароля, связанные с работой виртуальной клавиатуры от электронного устройства.

Блок сравнения выполнен с возможностью сравнения введенного пароля с заранее установленным паролем в ответ на запрос подтверждения пароля от устройства ввода,.

Другая задача раскрытия состоит в обеспечении компьютерной системы, содержащей устройство проверки пароля.

В соответствии с раскрытием, компьютерная система содержит электронное устройство, устройство ввода и устройство проверки пароля.

Электронное устройство содержит компьютерный модуль, исполняющий операционную систему (OS), установленную с прикладной управляющей программой, и модуль отображения, электрически соединенный с компьютерным модулем. Устройство проверки пароля является независимым автономным устройством, в котором хранится заранее установленный пароль и которое электрически подключается между устройством ввода и электронным устройством.

Устройство проверки пароля выполнено с возможностью формирования, в ответ на запрос ввода пароля от прикладной управляющей программы, данных изображения, связанных с виртуальной клавиатурой, и передачи данных изображения компьютерному модулю, так что компьютерный модуль управляет модулем отображения для отображения на нем виртуальной клавиатуры.

Компьютерный модуль выполнен с возможностью формирования данных пароля в ответ на операцию виртуальной клавиатуры и передачи данных пароля на устройство проверки пароля и устройство проверки пароля выполнено с возможностью создания входного пароля в соответствии с данными пароля.

Устройство проверки пароля выполнено с возможностью сравнения входного пароля с заранее установленным паролем в ответ на запрос подтверждения пароля от устройства ввода.

Краткое описание чертежей

Другие признаки и преимущества раскрытия станут очевидны из последующего подробного описания варианта осуществления со ссылкой на сопроводительные чертежи, на которых:

фиг. 1 - блок-схема варианта осуществления, показывающая вариант осуществления компьютерной системы, соответствующей раскрытию;

фиг. 2 - блок-схема последовательности выполнения операций способа, осуществляемого устройством проверки пароля компьютерной системы;

фиг. 3 - блок-схема последовательности выполнения операций взаимодействия между устройством проверки пароля и прикладной управляющей программой для получения данных пароля;

фиг. 4 - блок-схема последовательности выполнения операций взаимодействия между устройством проверки пароля и прикладной управляющей программой для проверки запроса подтверждения пароля; и

фиг. 5 и 6 - соответственно показывают виртуальную клавиатуру.

Подробное описание раскрытия

На фиг. 1 показана компьютерная система, соответствующая варианту осуществления раскрытия. Компьютерная система содержит электронное устройство 1, устройство 3 проверки пароля и устройство 4 ввода.

Электронное устройство 1 может быть реализовано, используя персональный компьютер, ноутбук, планшетный компьютер и т.д. Электронное устройство 1 содержит основное устройство 111 памяти, компьютерный модуль 112, основной модуль 2 ввода и модуль 5 отображения.

Основное устройство 111 памяти и компьютерный модуль 112 могут быть компонентами, интегрированными в материнскую плату 11.

Основное устройство 111 памяти хранит операционную систему (OS), которая устанавливается с прикладной управляющей программой 12. Компьютерный модуль 112 может быть реализован, используя центральный процессор (CPU), и выполняется с возможностью исполнения OS. Основной модуль 2 ввода может быть реализован, используя мышь, клавиатуру, сенсорный экран, сенсорную панель или их комбинацию. Основной модуль 2 ввода и модуль 5 отображения электрически соединяются с компьютерным модулем 112 и управляются с помощью OS.

Устройство 3 проверки пароля является независимым автономным устройством и может быть реализовано, используя чип, управляемый встроенным программным обеспечением. Устройство 3 проверки пароля содержит блок 31 формирования виртуальных клавиш, блок 32 сравнения, блок 33 запоминающего устройства и процессорный блок 34.

Устройство 4 ввода присоединяется к устройству 3 проверки пароля. Другими словами, устройство 3 проверки пароля электрически подключается между устройством 4 ввода и электронным устройством 1. Устройство 4 ввода может быть реализовано, используя, например, клавиатуру, мышь, переключатель, сенсорную панель или их комбинацию. Соединение между устройством 3 проверки пароля и устройством 3 ввода может быть проводным соединением или беспроводным соединением (например, использующим связь в ближнем поле (NFC), Wi-Fi, Bluetooth (BT), инфракрасное излучение (IR) и т.д.).

При работе, когда требуется проверить пароль (например, когда пользователь пытается получить доступ к определенному защищенному контенту, хранящемуся в основном запоминающем устройстве 111, или исполнить определенный защищенный паролем признак OS через основной модуль 2 ввода и/или через устройство 4 ввода), прикладная управляющая программа 12 формирует запрос ввода пароля и передает запрос ввода пароля на устройство 3 проверки пароля.

В ответ блок 31 формирования виртуальных клавиш устройства 3 проверки пароля формирует данные изображения, связанные с виртуальной клавиатурой. Блок 31 формирования виртуальных клавиш затем передает данные изображения электронному устройству 1.

Компьютерный модуль 112 использует данные изображения для управления модулем 5 отображения, чтобы отображать на нем виртуальную клавиатуру (один из примеров показан на фиг. 5), и дает команду пользователю предоставить входной пароль, используя основной модуль 2 ввода или устройство 4 ввода. В этом варианте осуществления входной пароль содержит последовательность чисел.

В одном из примеров, устройство 4 ввода может не содержать все функциональные возможности основного модуля 2 ввода (например, устройство ввода может быть простым переключателем, выполненным с возможностью передачи двоичного сигнала) и входной пароль вводится, используя основной модуль 2 ввода.

Каждый раз, когда какое-либо число вводится, используя основной модуль 2 ввода (посредством операции на виртуальной клавиатуре, такой как щелчок мышью по местоположению нажатия на виртуальной клавиатуре, которое соответствует

определенному числу, или используя сенсорный экран, чтобы позволить пользователю напрямую "коснуться" определенного числа), компьютерный модуль 112 получает набор координат местоположения нажатия и посылает набор координат на устройство 3 проверки пароля. В то же время, компьютерный модуль 112 управляет модулем 5 отображения, чтобы отображать случайный символ в поле прохождения ввода на виртуальной клавиатуре, указывающей, какое число было введено. В примере, показанном на фиг. 5, может использоваться символ (*).

Используя набор координат, процессорный блок 34 устройства 3 проверки пароля способен определять буквенно-цифровой символ, который отображается на виртуальной клавиатуре и который соответствует местоположению нажатия. Буквенно-цифровой символ затем сохраняется процессорным блоком 34 для составления входного пароля, впоследствии располагая буквенно-цифровые символы в порядке последовательности местоположений символов.

После того, как весь входной пароль был предоставлен, от пользователя требуют предоставить запрос подтверждения пароля, используя устройство 4 ввода. В настоящем примере запрос подтверждения пароля имеет форму двоичного сигнала.

В ответ на запрос подтверждения пароля от устройства 4 ввода, процессорный блок 34 сравнивает введенный пароль и заранее установленный пароль, ранее сохраненный в блоке 33 запоминающего устройства.

В этом примере после приема от устройства 4 ввода данных операции процессорный блок 34 формирует и сохраняет событие нажатия в блоке 33 запоминающего устройства (в качестве знака для доказательства, что источником данных операции является устройство 4 ввода). Процессорный блок 34 сравнивает введенный пароль с заранее установленный пароль, только когда событие нажатия сохранено в блоке 33 запоминающего устройства. После сравнения процессорным блоком 34 введенного пароля и заранее установленного пароля событие нажатия стирается (так что последующая попытка получения доступа, например, к защищенным паролем признакам, снова потребует этой процедуры подтверждения, содержащей запрос подтверждения пароля от устройства 4 ввода).

Заметим, что OS, исполняемая компьютерным модулем 112, может быть атакована хакерами и поэтому передача данных (в том числе, пароля, введенного, используя основной модуль 2 ввода) через OS может быть получена третьей стороной, имеющей несанкционированный доступ к OS, используя, например, удаленно управляемый хост-компьютер.

В результате, в этом варианте осуществления устройство 3 проверки пароля выполнено с возможностью считать запрос подтверждения пароля действительным и предпринимать последующие действия, только когда запрос подтверждения пароля принимается непосредственно от устройства 4 ввода, которое является автономным устройством и не управляется OS. То есть, когда третье лицо пытается получить доступ к защищенному паролем признаку и посылает запрос подтверждения пароля, используя устройство, отличное устройства 4 ввода, устройство 3 проверки пароля не будет переходить к сравнению введенного пароля с заранее установленным паролем.

В этом случае, даже если заранее установленный пароль становится известен третьему лицу, доступ к защищенным паролем признакам без использования устройства 4 ввода все еще блокируется

Когда определено, что входной пароль подтверждается заранее установленным паролем, устройство 3 проверки пароля проверяет, что введенный пароль правилен (и может, соответственно, позволить предоставить доступ к определенным защищенным

паролем признакам). В противном случае, когда определено, что входной пароль не подтверждается заранее установленным паролем, устройство 3 проверки пароля определяет, что входной пароль неправилен и ко всем признакам, защищенным паролем, соответственно, запрещается доступ.

В другом примере настоящего изобретения устройство 4 ввода содержит функциональные возможности основного модуля 2 ввода. То есть, входной пароль может вводиться, используя устройство 4 ввода и основной модуль 2 ввода не используется для цели введения входного пароля. В таком случае, определение входного пароля делается следующим образом.

После приема от устройства 4 ввода данных операции, связанных с операцией устройства 4 ввода на виртуальной клавиатуре, процессорный блок 34 формирует и сохраняет в блоке 33 запоминающего устройства событие нажатия.

Далее данные операции направляются прикладной управляющей программе 12, поэтому прикладная управляющая программа 12 выполнена с возможностью получения, соответственно, множества наборов координат местоположений нажатий на виртуальной клавиатуре в соответствии с данными операции. Прикладная управляющая программа 12 затем посылает наборы координат на устройство 3 проверки пароля в качестве данных пароля.

Устройство 3 проверки пароля определяет буквенно-цифровые символы, которые отображаются на виртуальной клавиатуре соответственно в местоположениях нажатий в соответствии с наборами координат, только когда событие нажатия сохранено в блоке 33 запоминающего устройства. После этого событие нажатия стирается.

Наборы координат могут кодироваться в данные пароля перед тем, как будут передаваться устройству 3 проверки пароля и, соответственно, устройство 3 проверки пароля декодирует данные пароля, чтобы извлечь наборы координат перед тем, как из них определяются буквенно-цифровые символы.

В этом примере виртуальная клавиатура, отображаемая на устройстве 4 ввода, содержит кнопку подтверждения (смотрите фиг. 6) и запрос подтверждения пароля имеет форму местоположения нажатия на виртуальной клавиатуре (то есть, от пользователя требуется работать с устройством 4 ввода, чтобы "нажимать" на кнопку подтверждения для введения запроса подтверждения пароля).

Подобно операциям, относящимся к приему входного пароля, после приема от устройства 4 ввода данных операции, которые связаны с операцией устройства 4 ввода на виртуальной клавиатуре, процессорный блок 34 формирует и сохраняет событие нажатия в блоке 33 запоминающего устройства.

Данные операции затем направляются прикладной управляющей программе 12, поэтому прикладная управляющая программа 12 выполнена с возможностью получения набора координат местоположения нажатия на виртуальной клавиатуре в соответствии с данными операции, и посылки набора координат на устройство 3 проверки пароля.

Устройство 3 проверки пароля выполнено с возможностью проверки, что запрос подтверждения пароля подлинен, только когда местоположение нажатия, соответствующее набору координат, соответствует кнопке подтверждения и когда событие нажатия хранится в блоке 33 запоминающего устройства. С помощью подлинного запроса подтверждения пароля устройство 3 проверки пароля сравнивает введенный пароль с заранее установленным паролем, после чего событие нажатия удаляется.

Операции, выполняемые компьютерной системой, могут быть выражены как способ проверки вводимого пароля. Этапы способа показаны на фиг. 2, сопровождающем

последующее описание.

На этапе 601 прикладная управляющая программа 12, исполняемая компьютерным модулем 112, передает запрос ввода пароля устройству 3 проверки пароля.

На этапе 602 устройство 3 проверки пароля формирует данные изображения, связанные с виртуальной клавиатурой, и передает данные изображения к компьютерному модулю 112, так чтобы компьютерный модуль 112 управлял модулем 5 отображения для отображения на нем виртуальной клавиатуры.

На этапе 603 введенный пароль принимается. В ответ компьютерный модуль 112 передает данные пароля, связанные с операцией виртуальной клавиатуры, устройству 3 проверки пароля. Конкретно, данные пароля содержат последовательность местоположений нажатий на виртуальной клавиатуре.

На этапе 604 устройство 3 проверки пароля составляет входной пароль в соответствии с данными пароля. Конкретно, для каждого из местоположений нажатия устройство 3 проверки пароля определяет буквенно-цифровой символ, который отображается на виртуальной клавиатуре и который соответствует местоположению нажатия. Затем устройство 3 проверки пароля составляет входной пароль, располагая буквенно-цифровые символы в порядке последовательности местоположений нажатий.

На этапе 605 устройство 3 проверки пароля проверяет источник запроса подтверждения пароля. Когда проверено, что запрос подтверждения пароля послан от устройства 4 ввода, последовательность выполнения операций переходит к этапу 606. В противном случае, последовательность выполнения операций заканчивается.

На этапе 606 устройство 3 проверки пароля сравнивает входной пароль с заранее установленным паролем.

Когда на этапе 606 определено, что входной пароль соответствует заранее установленному паролю, устройство 3 проверки пароля проверяет, что входной пароль правилен (этап 607). Когда на этапе 606 определено, что входной пароль не соответствует заранее установленному паролю, паролю, устройство 3 проверки пароля определяет, что входной пароль неправилен (этап 608).

Как показано на фиг. 3, в примере, где устройство 4 ввода используется для введения входного пароля, операции, содержащиеся на этапе 603, выполняются следующим образом.

На подэтапе 703 устройство 3 проверки пароля формирует и сохраняет в нем событие нажатия.

На подэтапе 704 устройство 3 проверки пароля направляет данные операции прикладной управляющей программе 12.

На подэтапе 705 прикладная управляющая программа 12 соответственно получает множество наборов координат для местоположений нажатий на виртуальной клавиатуре, соответствующих данным операции, и посылает наборы координат на устройство 3 проверки пароля в качестве данных пароля. Наборы координат могут быть закодированы в данные пароля перед их передачей устройству 3 проверки пароля и, соответственно, устройство 3 проверки пароля декодирует данные пароля, чтобы извлечь наборы координат перед тем, как определить буквенно-цифровые символы.

Затем на этапе 604, на подэтапе 706, событие нажатия удаляется.

Как показано на фиг. 4, в этом примере операции, содержащиеся на этапе 605, выполняются следующим способом.

На подэтапе 801 устройство 3 проверки пароля формирует и сохраняет событие нажатия.

На подэтапе 802 устройство 3 проверки пароля направляет данные операции

прикладной управляющей программе 12.

На подэтапе 803 прикладная управляющая программа 12 получает набор координат для местоположения нажатия на виртуальной клавиатуре в соответствии с данными операции и посылает набор координат устройству 3 проверки пароля.

На подэтапе 804 устройство 3 проверки пароля определяет, что запрос подтверждения пароля был принят, только когда местоположение нажатия соответствует кнопке подтверждения и когда событие нажатия сохранено в устройстве 3 проверки пароля. Устройство 3 проверки пароля выполнено с возможностью удаления хранящегося в нем события нажатия после проверки, что, запрос подтверждения пароля был принят, и последовательность выполнения операций переходит к этапу 606. В противном случае, последовательность выполнения операций заканчивается.

Подводя итоги, компьютерная система и способ раскрытия обеспечивают путь дальнейшего улучшения защищенных паролем признаков в электронном устройстве 1, обеспечивая устройство 3 проверки пароля и устройство 4 ввода, которые не управляются OS, и в результате даже при том, что OS может быть похищена и заранее установленный пароль может быть известен третьему лицу, защищенные паролем признаки могут все же оставаться недоступными без физического получения доступа к устройству 3 проверки пароля и устройству 4 ввода.

Хотя раскрытие было описано в связи с тем, что считается примерным вариантом осуществления, следует понимать, что это раскрытие не ограничивается раскрытым вариантом осуществления, а предназначено охватывать различные устройства, содержащиеся в рамках духа и объема самой широкой интерпретации, чтобы охватить все такие модификации и эквивалентные устройства.

(57) Формула изобретения

1. Способ проверки входного пароля, осуществляемый устройством (3) проверки пароля, электрически подключенным между устройством (4) ввода данных и электронным устройством (4), причем электронное устройство (4) содержит компьютерный модуль (112), исполняющий операционную систему (OS), установленную с прикладной управляющей программой (12), и модуль (5) отображения, электрически соединенный с компьютерным модулем (112), и устройство (3) проверки пароля является независимым автономным устройством и хранит заранее установленный пароль, и упомянутый способ содержит этапы, на которых:

a) в ответ на запрос ввода пароля от прикладной управляющей программы (12) формируют данные изображения, связанные с виртуальной клавиатурой, и передают данные изображения к компьютерному модулю (112), так что компьютерный модуль (112) управляет модулем (5) отображения, чтобы отображать на нем виртуальную клавиатуру;

b) в ответ на операцию виртуальной клавиатуры формируют данные пароля и составляют входной пароль, соответствующий данным пароля; и

c) в ответ на запрос подтверждения пароля от устройства (4) ввода сравнивают входной пароль и заранее установленный пароль,

в котором данные пароля содержат последовательность местоположений нажатий на виртуальной клавиатуре и этап b) содержит подэтапы, на которых:

b1) для каждого из местоположений нажатий определяют буквенно-цифровой символ, отображаемый на виртуальной клавиатуре и соответствующий местоположению нажатия; и

b2) создают входной пароль, располагая буквенно-цифровые символы в порядке

следования местоположений нажатий; при этом

перед подэтапом b1) после приема от устройства (4) ввода данных операции, связанных с операцией устройства (4) ввода на виртуальной клавиатуре, формируют и сохраняют событие нажатия; и

посылают данные операции прикладной управляющей программе (12) и прикладная управляющая программа (12) выполнена с возможностью получения множества наборов координат, соответственно, для местоположений нажатий на виртуальной клавиатуре согласно данным операции и посылки наборов координат на устройство (3) проверки пароля в качестве данных пароля,

в котором на подэтапе b1) устройство (3) проверки пароля определяет буквенно-цифровые символы, соответственно отображаемые на виртуальной клавиатуре в местоположениях нажатий в соответствии с наборами координат, только когда событие нажатия сохранено в устройстве (3) проверки пароля,

в котором этап b) дополнительно содержит подэтап, следующий после подэтапа b2), для удаления из него события нажатия.

2. Способ по п. 1, в котором местоположения нажатий кодируются в данных пароля прикладной управляющей программой (12) и этап b) дополнительно содержит перед подэтапом b1) этап декодирования данных пароля, чтобы извлечь местоположения нажатий.

3. Способ по п. 1, в котором каждое из местоположений нажатий указывается набором координат.

4. Способ по п. 1, в котором наборы координат кодируются в данные пароля перед передачей устройству (3) проверки пароля и устройство (3) проверки пароля декодирует данные пароля, чтобы извлечь наборы координат перед определением буквенно-цифровых символов.

5. Способ по п. 1, в котором виртуальная клавиатура содержит кнопку подтверждения, запрос подтверждения пароля содержит местоположение нажатия на виртуальной клавиатуре и этап c) содержит подэтапы, на которых:

после приема от устройства (4) ввода данных операции, связанных с операцией устройства (4) ввода на виртуальной клавиатуре, формируют и сохраняют в нем событие нажатия;

посылают данные операции прикладной управляющей программе (12), и прикладная управляющая программа (12) выполнена с возможностью получения набора координат для местоположения нажатия на виртуальной клавиатуре в соответствии с данными операции и посылки набора координат устройству (3) проверки пароля;

определяют, что запрос подтверждения пароля был получен, только когда местоположение нажатия, соответствующее набору координат, соответствует кнопке подтверждения и когда событие нажатия сохранено в устройстве (3) проверки пароля; и

удаляют сохраненное событие нажатия.

6. Способ по п. 1, который после сравнения входного пароля и заранее установленного пароля дополнительно содержит этапы, на которых:

когда на этапе c) определено, что входной пароль соответствует заранее установленному паролю, подтверждают, что входной пароль правилен; и

когда на этапе c) определено, что входной пароль не соответствует заранее установленному паролю, принимают решение, что входной пароль является неправильным.

7. Компьютерная система, содержащая:

электронное устройство (4), содержащее

компьютерный модуль (112), исполняющий операционную систему (OS), установленную с прикладной управляющей программой (12), и

модуль (5) отображения, электрически соединенный с упомянутым компьютерным модулем (112);

устройство (4) ввода; и

устройство (3) проверки пароля, являющееся независимым автономным устройством, в котором хранится заранее установленный пароль и которое электрически подключается между упомянутым устройством (4) ввода и упомянутым электронным устройством (4);

в которой:

упомянутое устройство (3) проверки пароля выполнено с возможностью формирования, в ответ на запрос ввода пароля от прикладной управляющей программы (12), данных изображения, связанных с виртуальной клавиатурой и передачи данных изображения упомянутому компьютерному модулю (112), так что упомянутый компьютерный модуль (112) управляет упомянутым модулем (5) отображения для отображения на нем виртуальной клавиатуры;

упомянутый компьютерный модуль (112) выполнен с возможностью формирования, в ответ на операцию виртуальной клавиатуры, данных пароля и передачи данных пароля упомянутому устройству (3) проверки пароля и упомянутое устройство (3) проверки пароля выполнено с возможностью составления входного пароля в соответствии с данными пароля; и

упомянутое устройство (3) проверки пароля выполнено с возможностью сравнения, в ответ на запрос подтверждения пароля от упомянутого устройства (4) ввода, входного пароля с заранее установленным паролем.

8. Компьютерная система по п. 7, в которой:

данные пароля, сформированные упомянутым компьютерным модулем (112), содержат последовательность местоположений нажатий на виртуальной клавиатуре;

для каждого из местоположений нажатий упомянутое устройство (3) проверки пароля выполнено с возможностью определения буквенно-цифрового символа, который отображается на виртуальной клавиатуре и который соответствует местоположению нажатия; и

упомянутое устройство (3) проверки пароля составляет входной пароль, выстраивая буквенно-цифровые символы в порядке последовательности местоположений нажатий.

9. Компьютерная система по п. 8, в которой упомянутый компьютерный модуль (112) дополнительно выполнен с возможностью кодирования местоположений нажатий в данные пароля перед передачей данных пароля упомянутому устройству (3) проверки пароля и упомянутое устройство (3) проверки пароля выполнено с возможностью декодирования данных пароля для извлечения местоположений нажатий.

10. Компьютерная система по п. 8, в которой каждое из местоположений нажатий указывается набором координат.

11. Компьютерная система по п. 8, в которой:

упомянутое устройство (3) проверки пароля выполнено с возможностью формирования и сохранения в нем события нажатия после приема связанных с операцией упомянутого устройства (4) ввода на виртуальной клавиатуре данных операции от упомянутого устройства (4) ввода перед посылкой данных операции упомянутому компьютерному модулю (112);

упомянутый компьютерный модуль (112) выполнен с возможностью получения

множества наборов координат соответственно для местоположений нажатий на виртуальной клавиатуре в соответствии с данными операции и посылки наборов координат упомянутому устройству (3) проверки пароля в качестве данных пароля; и

упомянутое устройство (3) проверки пароля выполнено с возможностью удаления события нажатия после создания входного пароля.

12. Компьютерная система по п. 11, в которой упомянутый компьютерный модуль (112) выполнен с возможностью кодирования наборов координат в данные пароля перед передачей данных пароля упомянутому устройству (3) проверки пароля и упомянутое устройство (3) проверки пароля выполнено с возможностью декодирования данных пароля для извлечения наборов координат перед определением буквенно-цифровых символов.

13. Компьютерная система по п. 7, в которой:

виртуальная клавиатура, отображаемая упомянутым модулем (5) отображения, содержит кнопку подтверждения и запрос подтверждения пароля содержит определение местоположения нажатия на виртуальной клавиатуре;

упомянутое устройство (3) формирования пароля выполнено с возможностью формирования и сохранения в нем события нажатия после приема от упомянутого устройства (4) ввода данных операции, связанных с операцией упомянутого устройства (4) ввода на виртуальной клавиатуре, и перед посылкой данных операции упомянутому компьютерному модулю (112); и

упомянутый компьютерный модуль (112) выполнен с возможностью получения набора координат местоположения нажатия на виртуальной клавиатуре в соответствии с данными операции и посылки набора координат упомянутому устройству (3) проверки пароля;

упомянутое устройство (3) проверки пароля выполнено с возможностью проверки, что запрос подтверждения пароля был принят, только когда местоположение нажатия, соответствующее набору координат, соответствует кнопке подтверждения и когда событие нажатия сохранено в упомянутом устройстве (3) проверки пароля; и

упомянутое устройство (3) проверки пароля выполнено с возможностью удаления хранящегося в нем события удаления после проверки, что запрос подтверждения пароля был принят.

14. Компьютерная система по п. 8, в которой для каждого из местоположений нажатий упомянутый компьютерный модуль (112) выполнен с возможностью передачи команды упомянутому компьютерному модулю (112) и в ответ упомянутый компьютерный модуль (112) выполняется с возможностью управления упомянутым модулем (5) отображения, чтобы отображать случайный символ на поле продвижения ввода виртуальной клавиатуры.

15. Компьютерная система по п. 7, в которой:

упомянутое устройство (3) проверки пароля выполнено с возможностью проверки, что пароль правильный, когда определено, что входной пароль соответствует заранее установленному паролю; и

упомянутое устройство (3) проверки пароля выполнено с возможностью проверки, что пароль неправильный, когда определено, что входной пароль не соответствует заранее установленному паролю.

16. Компьютерная система по п. 7, в которой упомянутое устройство (4) ввода содержит по меньшей сенсорную панель или мышь.

17. Устройство (3) проверки пароля для проверки входного пароля, причем упомянутое устройство (3) проверки пароля является независимым автономным

устройством и электрически подключается между устройством (4) ввода и электронным устройством (4) и упомянутое устройство (3) проверки пароля содержит:

блок (31) формирования виртуальных клавиш, который в ответ на запрос ввода пароля от электронного устройства (4) выполняется с возможностью формирования данных изображения, соответствующих виртуальной клавиатуре, и передачи данных изображения на электронное устройство (4);

блок (33) запоминающего устройства (33), в котором хранится заранее установленный пароль;

процессорный блок (34), который в ответ на данные пароля, связанные с операцией виртуальной клавиатуры от электронного устройства (4), выполняется с возможностью составления входного пароля в соответствии с данными пароля, и

модуль (32) сравнения, который в ответ на запрос подтверждения пароля от устройства (4) ввода выполняется с возможностью сравнения входного пароля и заранее установленного пароля.

18. Устройство (3) проверки пароля по п. 17, где данные пароля содержат последовательность местоположений нажатий на виртуальной клавиатуре, в котором:

для каждого из местоположений нажатий упомянутый процессорный блок (34) выполняется с возможностью определения буквенно-цифрового символа, который отображается на виртуальной клавиатуре и который соответствует местоположению нажатия; и

упомянутый процессорный блок (34), выполненный с возможностью составления входного пароля, располагая буквенно-цифровые символы в порядке последовательности местоположений нажатий.

19. Устройство (3) проверки пароля по п. 18, в котором местоположение нажатия кодируется в данных пароля электронным устройством (4) и упомянутый процессорный блок (34) выполнен с возможностью декодирования данных пароля для извлечения местоположений нажатий.

20. Устройство (3) проверки пароля по п. 18, в котором:

после приема от устройства (4) ввода данных операции, связанных с операцией устройства (4) ввода на виртуальной клавиатуре, упомянутый процессорный блок (34) выполняется с возможностью формирования события нажатия и сохранения события нажатия в упомянутом блоке (33) запоминающего устройства;

упомянутый процессорный блок (34), дополнительно выполненный с возможностью посылки данных операции электронному устройству (4), так что электронное устройство (4) выполнено с возможностью получения множества наборов координат соответственно для местоположений нажатий на виртуальной клавиатуре в соответствии с данными операции и посылки набора координат упомянутому устройству (3) проверки пароля в качестве данных пароля;

упомянутый процессорный блок (34) определяет буквенно-цифровые символы, которые отображаются на виртуальной клавиатуре соответственно в местоположениях нажатий в соответствии с наборами координат, только когда событие нажатия сохранено в упомянутом блоке (33) запоминающего устройства; и

упомянутый процессорный блок (34) выполнен с возможностью удаления события нажатия после создания входного пароля.

21. Устройство (3) проверки пароля по п. 19, в котором наборы координат кодируются в данные пароля перед тем, как передаваться упомянутому устройству (3) проверки пароля, и упомянутый процессорный блок (34) декодирует данные пароля, чтобы извлечь наборы координат перед определением буквенно-цифровых символов.

22. Устройство (3) проверки пароля по п. 17, виртуальная клавиатура, содержащая подтверждающуюся кнопку, запрос подтверждения пароля, содержащий определение местоположения нажатия на виртуальной клавиатуре, в которых:

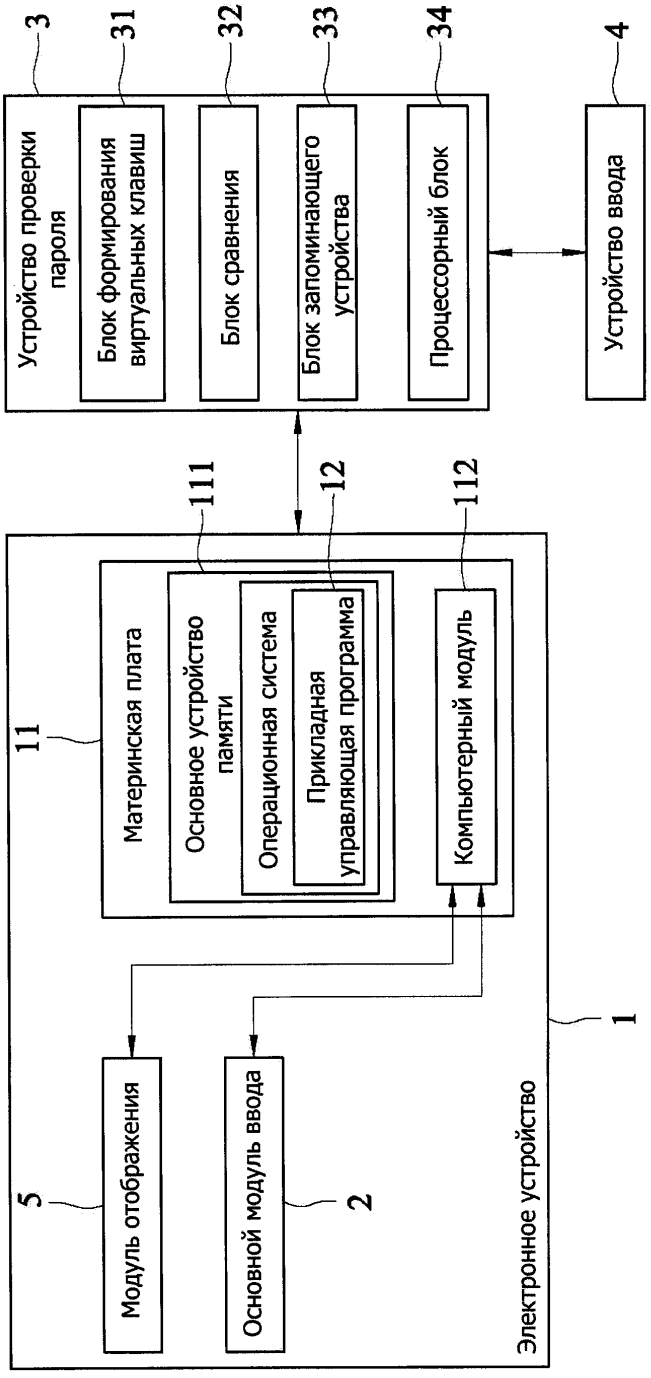
после приема от устройства (4) ввода данных операции, связанных с операцией устройства (4) ввода на виртуальной клавиатуре, упомянутый процессорный блок (34) выполняют с возможностью формирования события нажатия и сохранения события нажатия в упомянутом блоке (33) запоминающего устройства;

упомянутый процессорный блок (34) дополнительно выполняют с возможностью посылки данных операции электронному устройству (4), так что электронное устройство (4) настраивают с возможностью получения набора координат для местоположения нажатия на виртуальной клавиатуре в соответствии с данными операции и посылки наборов координат устройству (3) проверки пароля;

упомянутый процессорный блок (34) выполняют с возможностью проверки, что запрос подтверждения пароля был принят, только когда местоположения нажатия, соответствующее набору координат, соответствует кнопке подтверждения и когда событие нажатия хранится в упомянутом блоке (33) запоминающего устройства (33); и

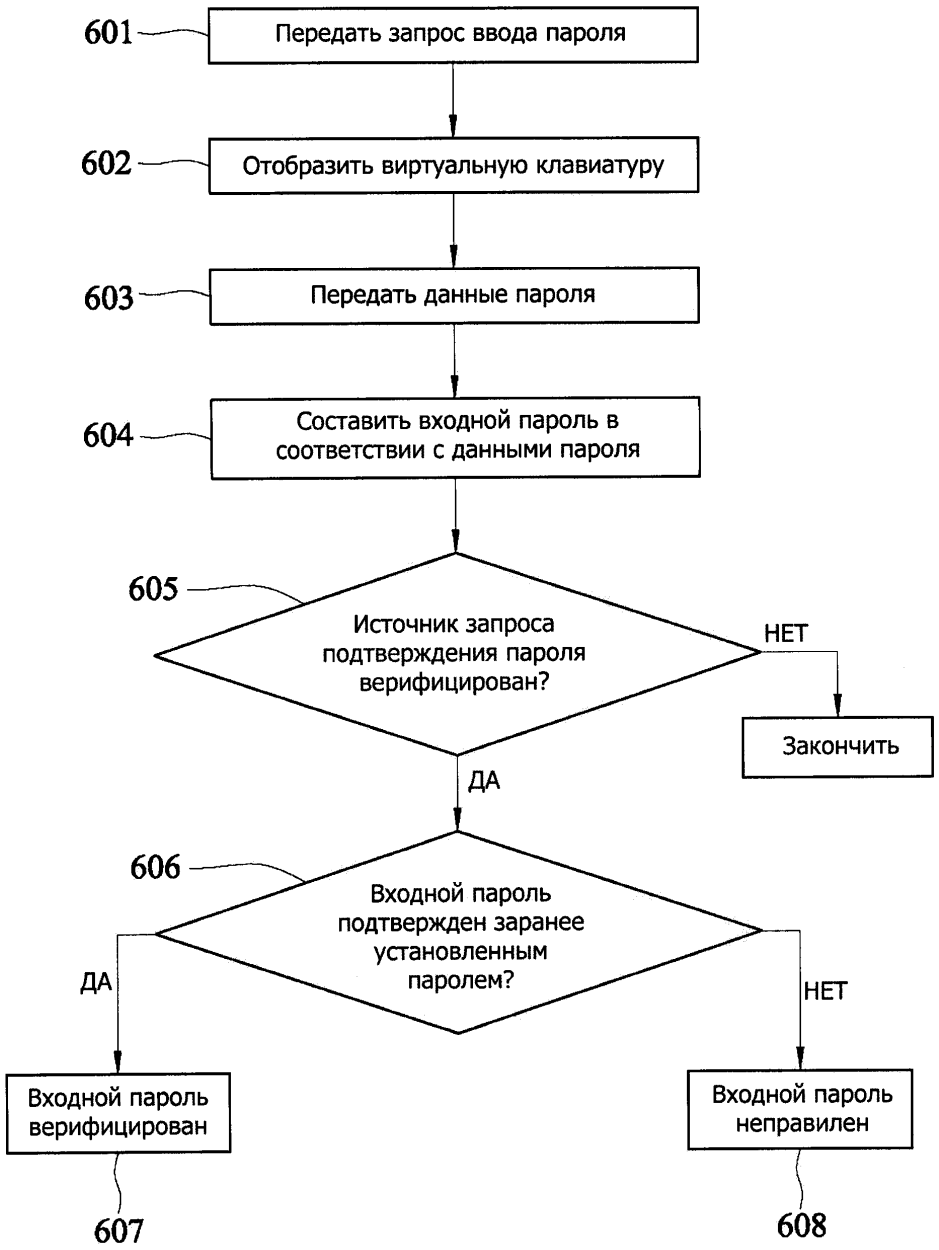
после проверки, что запрос подтверждения пароля был принят, упомянутый процессорный блок (34) выполняют с возможностью удаления хранящегося в нем события нажатия.

1


3
31
32
33
34
4
Устройство проверки пароля
Блок формирования виртуальных клавиш
Блок сравнения
Блок запоминающего устройства
Процессорный блок
Устройство ввода
111
12
112
11
Материнская плата
Основное устройство памяти
Операционная система
Прикладная управляющая программа
Компьютерный модуль
5
2
1
Модуль отображения
Основной модуль ввода
Электронное устройство

Фиг. 1

2


601
Передать запрос ввода пароля
602
Отобразить виртуальную клавиатуру
603
Передать данные пароля
604
Составить входной пароль в соответствии с данными пароля
605
Источник запроса подтверждения пароля верифицирован?
НЕТ
Закончить
ДА
606
Входной пароль подтвержден заранее установленным паролем?
ДА
НЕТ
Входной пароль верифицирован
Входной пароль неправилен
607
608

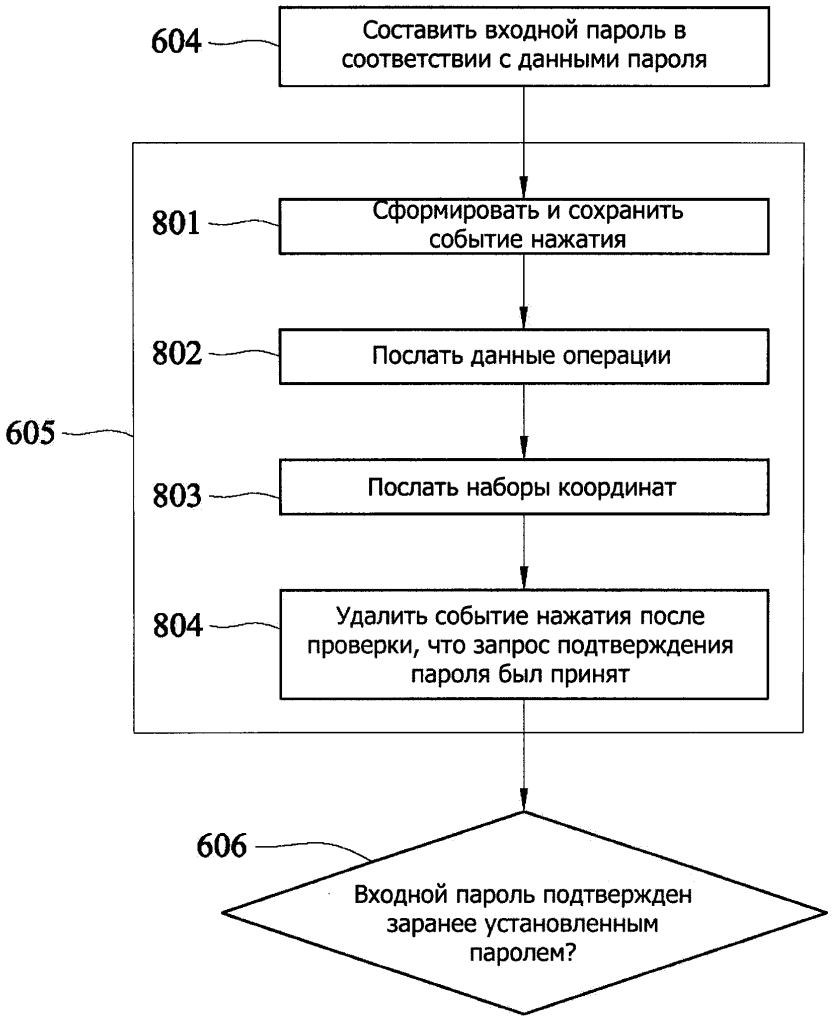
Фиг. 2

3

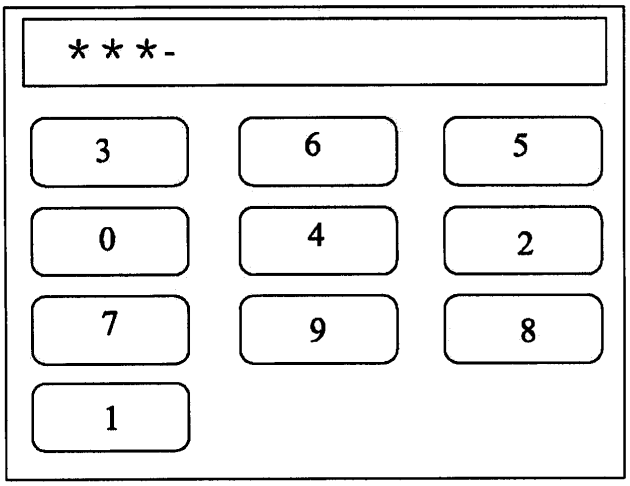

602
Отобразить виртуальную клавиатуру
703
Сформировать и сохранить событие нажатия
603
704
Послать данные операции
705
Послать наборы координат в качестве данных пароля
604
Составить входной пароль в соответствии с данными пароля
706
Удалить событие нажатия после составления входного пароля

Фиг. 3

4

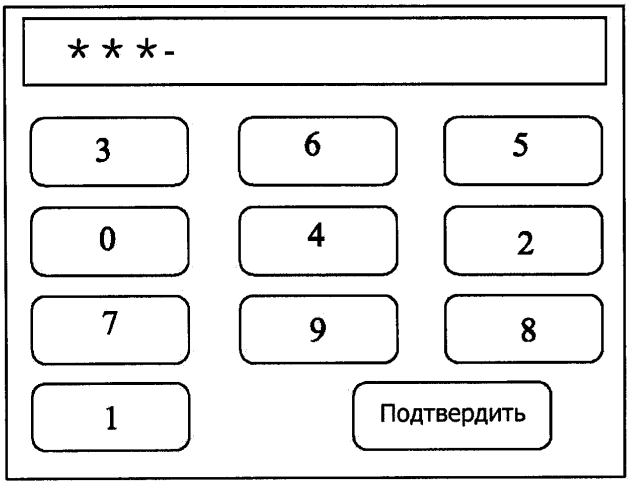

604
Составить входной пароль в соответствии с данными пароля
801
Сформировать и сохранить событие нажатия
802
Послать данные операции
605
803
Послать наборы координат
804
Удалить событие нажатия после проверки, что запрос подтверждения пароля был принят
606
Входной пароль подтвержден заранее установленным паролем?

Фиг. 4



Фиг. 5

6



Фиг. 6