



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2012117895/08, 30.09.2009

(24) Дата начала отсчета срока действия патента:
30.09.2009

Приоритет(ы):

(22) Дата подачи заявки: 30.09.2009

(43) Дата публикации заявки: 10.11.2013 Бюл. № 31

(45) Опубликовано: 20.11.2014 Бюл. № 32

(56) Список документов, цитированных в отчете о поиске: US 2002/0181747 A1, 05.12.2002. US 6393139 B1, 21.05.2002. JP 2007-189395 A, 26.07.2007. US 2007/0140530 A1, 21.06.2007. RU 2338258 C2, 10.11.2008. RU 2369025 C2, 27.09.2009

(85) Дата начала рассмотрения заявки РСТ на национальной фазе: 02.05.2012

(86) Заявка РСТ:
CN 2009/001114 (30.09.2009)

(87) Публикация заявки РСТ:
WO 2011/038533 (07.04.2011)

Адрес для переписки:

109012, Москва, ул. Ильинка, 5/2, ООО
"Союзпатент"

(72) Автор(ы):

**ХУАН Цзоу (CN),
ЧЖАН Цюньчжун (CN),
ГУЙ Кай (CN),
ТОБИАС М. Коленберг (US)**

(73) Патентообладатель(и):

ИНТЕЛ КОРПОРЕЙШН (US)

(54) ПОВЫШЕНИЕ БИОМЕТРИЧЕСКОЙ ЗАЩИЩЕННОСТИ СИСТЕМЫ

(57) Реферат:

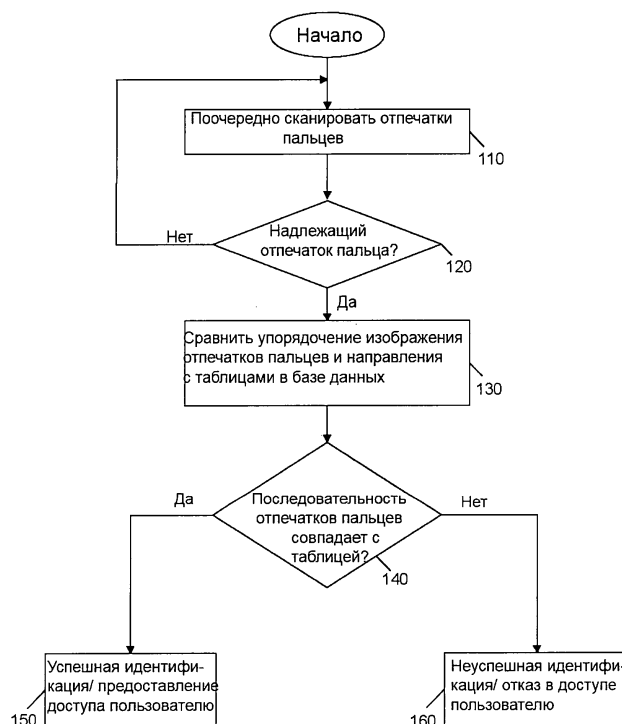
Изобретение относится к средствам для осуществления доступа к обрабатывающей системе. Техническим результатом является повышение надежности доступа к обрабатывающей системе. Способ доступа к обрабатывающей системе содержит этапы, на которых: принимают упорядоченную последовательность вводов биометрических данных от пользователя через биометрический датчик, связанный с обрабатывающей системой; определяют наличие совпадения каждого из вводов биометрических данных упорядоченной последовательности с соответствующей записью,

хранящейся в таблице энергонезависимого запоминающего устройства обрабатывающей системы, при этом таблица включает в себя сохраненную упорядоченную последовательность вводов биометрических данных, соответствующую комбинации пароля пользователя; и при наличии совпадения предоставляют пользователю доступ к обрабатывающей системе, а при отсутствии совпадения не допускают доступ пользователя к обрабатывающей системе, при этом каждый из вводов биометрических данных упорядоченной последовательности соответствует различному

пальцу пользователя и элементу комбинации для пароля, выбранной пользователем, причем первый палец пользователя соответствует первому алфавитно-цифровому символу,

выбранному пользователем, а второй палец пользователя соответствует второму алфавитно-цифровому символу, выбранному пользователем. 3 н. и 17 з.п. ф-лы, 6 ил.

100



Фиг. 4

RU 2 5 3 3 6 5 4 C 2

RU 2 5 3 3 6 5 4 C 2



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(51) Int. Cl.
G06F 17/00 (2006.01)
G06K 9/00 (2006.01)

(12) **ABSTRACT OF INVENTION**

(21)(22) Application: 2012117895/08, 30.09.2009
 (24) Effective date for property rights: 30.09.2009
 Priority:
 (22) Date of filing: 30.09.2009
 (43) Application published: 10.11.2013 Bull. № 31
 (45) Date of publication: 20.11.2014 Bull. № 32
 (85) Commencement of national phase: 02.05.2012
 (86) PCT application: CN 2009/001114 (30.09.2009)
 (87) PCT publication: WO 2011/038533 (07.04.2011)
 Mail address: 109012, Moskva, ul. Il'inka, 5/2, OOO "Sojuzpatent"

(72) Inventor(s):
KhUAN Tszou (CN),
ChZhAN Tsjun'chzhun (CN),
GUJ Kaj (CN),
TOBIAS M. Kolenberg (US)
 (73) Proprietor(s):
INTEL KORPOREJShN (US)

RU 2 533 654 C2

(54) **IMPROVING BIOMETRIC SECURITY OF SYSTEM**

(57) Abstract:

FIELD: physics, computer engineering.

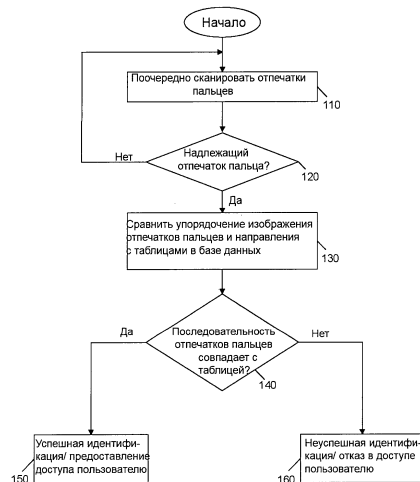
SUBSTANCE: invention relates to means of accessing a processing system. The method of accessing a processing system comprises steps of: receiving an ordered sequence of biometric data inputs from a user through a biometric sensor connected to the processing system; determining presence of a match of each of the biometric data inputs of the ordered sequence with a corresponding record stored in the table of non-volatile memory of the processing system, wherein the table includes the stored ordered sequence of biometric data inputs corresponding to a user password combination; and if there is match, providing the user with access to the processing system, and if there is no match, denying the user access to the processing system, wherein each of the biometric data inputs of the ordered sequence corresponds to a different finger of the user and an element of the password combination selected by the user, wherein the first finger of the user corresponds to the first alphanumeric character selected by the user, and the second finger of the user corresponds to the

second alphanumeric character selected by the user.

EFFECT: high reliability of access to a processing system.

20 cl, 6 dwg

100



Фиг. 4

RU 2 533 654 C2

Уровень техники

По мере того как пользователи систем, базирующихся на процессоре, возлагают повышенное доверие на эти системы и данные, сохраняющиеся в таких системах, значимость безопасности увеличивается. Чтобы обеспечить безопасность для таких систем, устанавливаются и используются для защиты доступа в общем к системе часто используемые пароли. Дополнительные пароли могут использоваться для защиты доступа к отдельным приложениям, файлам и доступа для взаимодействия с отдаленными источниками, такими как веб-сайты, доступные с помощью системы. Кроме того, дополнительно безопасность может быть обеспечена за счет зашифрования файлов и данных.

Однако когда имеется множество вариантов использования системы, пользователь может столкнуться с увеличивающимся количеством паролей, что может привести к потерям или путанице. Соответственно, некоторые пользователи выбирают общий пароль для множества различных типов приложений, что может в значительной степени подвергать риску безопасность.

Некоторые системы обеспечивают дополнительную безопасность в виде определенного типа биометрического датчика. Например, многие базирующиеся на процессоре устройства оборудуются датчиком отпечатков пальцев, который действует как устройство идентификации. Однако пользователь просто однократно размещает/сдвигает (в любом направлении перемещения) единственный палец на датчике и устройство выполняет процесс идентификации. Для многих целей, однако, этот вид механизма безопасности является недостаточно надежным.

Краткое описание чертежей

Фиг.1 является диаграммой, представляющей иллюстративное отображение цифр, в соответствии с одним вариантом осуществления настоящего изобретения.

Фиг.2 является диаграммой, которая показывает цифру и отображение соответствия направления перемещения к элементу пароля, в соответствии с одним вариантом осуществления настоящего изобретения.

Фиг.3 является схемой последовательности процесса для способа генерирования пароля в соответствии с одним вариантом осуществления настоящего изобретения.

Фиг.4 является схемой последовательности процесса для способа аутентификации пароля в соответствии с одним вариантом осуществления настоящего изобретения.

Фиг.5 является схемой последовательности процесса для способа генерирования пароля в соответствии с вариантом осуществления настоящего изобретения.

Фиг.6 является схемой последовательности процесса для способа аутентификации пароля в соответствии с другим вариантом осуществления настоящего изобретения.

Фиг.7 является блок-схемой системы для использования с одним вариантом осуществления изобретения.

Подробное описание

Варианты осуществления изобретения обеспечивают процесс идентификации при увеличенной безопасности, например, для систем, имеющих биометрический датчик, такой как датчик отпечатков пальцев. Чтобы выполнить идентификацию в соответствии с вариантом осуществления настоящего изобретения, пользователь может поместить различные пальцы (например, пальцы руки или пальцы ноги) в заданной последовательности или порядке на датчик. В некоторых вариантах применения пользователь может перемещать палец скользящим движением в различных направлениях, чтобы создать различные сканирующие последовательности, даже в случае использования того же самого пальца. Таким образом, идентификация является

более надежной, чем единый стиль ввода, даже в том случае, если какой-либо злоумышленник видит, какой палец пользователь помещает на датчик, он не может знать порядок и направление скользящего перемещения для определенного пальца, и таким образом, он не узнает пароль.

5 В различных вариантах применения упорядоченная последовательность различных цифр (с направлением перемещения или без него) может формировать пароль, также определяемый здесь как комбинация для пароля. Следует заметить, что в некоторых вариантах применения комбинация для пароля может не включать в себя какие-либо алфавитно-цифровые символы и вместо этого соответствует исключительно
10 последовательности цифр/перемещений. В других вариантах применения могут быть реализованы различные способы отображения биометрической информации и/или перемещений пользователя на элементы (например, алфавитно-цифровые значения) пароля. В то время как объем настоящего изобретения не ограничивается в этом отношении, в некоторых вариантах применения каждая из цифр пользователя может
15 отображать цифровой код таким образом, что десять пальцев соответствуют цифрам 0-9.

В одном варианте осуществления изобретения упорядоченная последовательность отпечатков пальцев, соответствующих различным цифрам, может быть использована, чтобы представлять чисто цифровой пароль. Таким образом, существующие цифровые
20 (и/или алфавитно-цифровые) пароли могут быть преобразованы в последовательность отпечатков пальцев, являющуюся уникальной для определенного пользователя. Таким образом, генерированные ранее пароли могут быть преобразованы в пароли на основе биометрических данных, чтобы улучшить надежность безопасности. Однако, как было описано выше, в других вариантах применения последовательность отпечатков пальцев
25 и перемещений пальцев могут сами по себе формировать пароль с жесткой последовательностью символов без отдельного соответствия символам клавиатуры.

Фиг.1 является диаграммой, представляющей иллюстративное отображение соответствия цифр, в соответствии с одним вариантом осуществления настоящего изобретения. В показанном на фиг.1 варианте осуществления изобретения отпечаток
30 пальца для каждого пальца левой и правой рук представляет цифру от 0 до 9. В то время как это является одним из примеров отображения соответствия, пользователь мог бы использовать любое представление для каждого отпечатка пальца, которое является уникальным только для него/нее. Таким образом, варианты осуществления изобретения обеспечивают более надежное физическое зашифрование для пароля, поскольку тот же самый пароль (например, 01234) будет иметь различные упорядоченные
35 последовательности для различных пользователей (например, соответствующие отпечаткам пальцев различных пользователей). Например, в одном варианте применения с отображением соответствия индивидуальных элементов пароля для различных пальцев пароль 01234 может соответствовать профилю идентификации единственной
40 последовательности отпечатков пальцев: большой палец, указательный палец, средний и безымянный палец на левой руке, как можно увидеть на фиг.1.

В других вариантах применения комбинация пальца и перемещения пользователя может отображать соответствующий элемент. Например, отпечаток большого пальца и перемещение в заданном направлении (например, слева направо или сверху вниз)
45 может отображать соответствие для заданного числа или другого символа. В некоторых вариантах применения пользователь может выбрать желаемые соответствия, в то время как в других вариантах осуществления изобретения соответствия могут быть заранее заданы системой. При использовании комбинации пальцев и направлений перемещения

(например, два направления на цифру) может быть получено 20 символов.

В варианте применения, в котором комбинация пальца и перемещения отображает соответствие значению, один пример соответствия может быть следующим: большой палец скользит сверху вниз и снизу вверх, что может соответствовать 0 и 1 (соответственно); указательный палец скользит сверху вниз и снизу вверх, что может соответствовать 2 и 3 (соответственно); и скольжение среднего пальца сверху вниз и снизу вверх представляет 4 и 5 (соответственно). Конечно, пользователь мог бы использовать различные пальцы, чтобы представлять различные элементы.

В вариантах применения фиг.2 отображение соответствия выполняется таким образом, что отображает как палец, так и направление перемещения как элемент пароля. Как видно на фиг.2, пользователь нажимает большим пальцем на датчик и совершает скользящее перемещение слева направо для отображения нулевого значения в качестве элемента пароля, в то время как перемещение справа налево устанавливается для значения единицы элемента пароля. В этом примере пароль 01010 может быть представлен перемещением большого пальца на датчике как (начиная от) слева, направо, налево, направо, налево и направо. Другие пальцы и/или другие перемещения могут соответствовать различным числам, или даже более специфическим значениям, которые являются уникальными для различных пользователей. Например, если пользователь говорит на американском языке жестов, то он или она могут выбрать использование набора пальцев и направлений, которые «произносят» что-нибудь многозначительное для пользователя. В целом, пользователь может выбрать любой жест пальцем из любого языка и использовать его для создания специфических, легко запоминающихся комбинаций, которые являются уникальными для пользователя. Программное обеспечение или программно-аппаратные средства принимают во внимание форму и размер поверхности датчика, и могут дать пользователю различные руководства для установки пароля. В одном варианте применения система может представлять пользователя со схемой музыкального инструмента, которая позволяет вводить комбинацию отпечатков пальцев и аккордов или их последовательностей. Или соответствие может быть реализовано за счет отображения диска наборного замка и отслеживания числа, на которое поворачивается циферблат, и какие пальцы (и как много пальцев) используются для поворачивания циферблата. В еще одном варианте применения, в котором биометрический датчик имеет трехмерную (3D) функцию, перемещения, которые скользят по стороне трехмерной поверхности, могут соответствовать отображению, например, кубика Рубика (Rubik™) или другой конструкции.

На фиг.3 показана схема последовательности процесса для способа генерирования пароля в соответствии с одним вариантом осуществления настоящего изобретения. Как показано на фиг.3, способ 10 может использоваться для отображения соответствия отпечатков пальцев пользователя и направлением перемещения или величиной перемещения, чтобы позволить генерирование комбинации пароля. Как показано на фиг.3, способ может начинаться с помощью инициирования фиксирования изображения отпечатков пальцев один за другим (блок 20). Например, система может инициировать модуль получения изображения отпечатка пальца, чтобы включить биометрический датчик для приема ввода отпечатка пальца. В одном варианте осуществления изобретения могут быть обеспечены отображения экрана, чтобы направлять пользователя посредством ввода с использованием различных пальцев и направлений перемещения. В частности, как можно увидеть на фиг.3 в блоке 30, система может запросить пользователя ввести упорядоченную последовательность отпечатков пальцев/

перемещений, которые соответствуют комбинации пароля. Система может затем сканировать отпечаток пальца заданной цифры и определить его направление перемещения (блок 40). Например, первый элемент комбинации пароля может соответствовать левому указательному пальцу, когда он перемещается через биометрический датчик сверху вниз. Отвечая на этот ввод, система может сохранить изображение отпечатка пальца и направление его перемещения в компоненте таблицы базы данных (блок 50). В одном варианте осуществления изобретения направление может сохраняться как метаданные, которые отмечают направление, в котором производится сканирование. Например, эта комбинация изображения отпечатка пальца и направления перемещения могут быть введены в первый компонент таблицы, который должен сохранять комбинацию пароля для этого конкретного пользователя и который сам по себе может быть частью базы данных паролей пользователя, сохраняемых в системе.

Как показано на фиг.3, в ромбовидной фигуре 60 может быть определено, была ли завершена комбинация пароля (ромбовидная фигура 60). Если нет, то управление переходит назад к блокам 40 и так далее для дополнительного получения отпечатка пальца/направления сканирования и его сохранения. Следует заметить, что таблица может таким образом включать в себя множество компонентов, каждый из которых должен сохранять соответствующее изображение отпечатка пальца и направление перемещения. В противном случае управление переходит к блоку 70, где таблица в базе данных может быть завершена. Соответственно, фиг.3 показывает способ получения изображений отпечатка пальца пользователя и направлений перемещения, которые соответствуют упорядоченной последовательности комбинации пароля. Следует заметить, что в этом варианте осуществления изобретения нет необходимости отображать соответствие этих изображений/перемещений каким-либо символам, доступным через клавиатуру. Вместо этого комбинация пароля может быть полностью физическим кодом, объединяющим отпечатки пальцев отдельного пользователя и направления вводимого перемещения.

Чтобы позволить пользователю получить доступ к системе, в которой он/она имеет одну или более сохраняемых комбинаций пароля, может быть использован такой способ, который описан по отношению к фиг.4. На фиг.4 показана схема последовательности процесса для способа аутентификации пароля в соответствии с одним вариантом осуществления настоящего изобретения. Как показано на фиг.4, способ 100 может начинаться сканированием одного за другим отпечатков пальцев (блок 110). Такое сканирование может быть выполнено пользователем, вводящим в определенном порядке отпечатки пальцев/направления, как это производилось для генерирования комбинации пароля, обсуждавшегося выше, по отношению к фиг.3. Для каждого ввода может быть определено, получен ли действительный отпечаток пальца (ромбовидная фигура 120). Если ответ положительный, то управление переходит к блоку 130. В противном случае управление переходит назад, к блоку 110, чтобы попытаться найти повторный ввод соответствующего отпечатка пальца. В некоторых вариантах применения система может обеспечить информацию для пользователя: был ли корректно принят каждый ввод, и может запросить повторный ввод в случае необходимости. Следует заметить, что в некоторых вариантах осуществления изобретения все отпечатки пальцев/направления могут быть просканированы перед продолжением процедуры в блоке 130. В некоторых вариантах осуществления изобретения ввод пользователя может обозначать, когда пользователь завершил ввод, который также может быть выбранным пользователем.

После получения отпечатков пальцев/направлений, сканирования/перемещения могут сравниваться с таблицами в базе данных (блок 130), где каждая таблица соответствует сохраняемой комбинации пароля для пользователя. Если более подробно, то в одном варианте применения первый ввод сканирования/направления перемещения может сравниваться с первым компонентом в каждой таблице, чтобы определить, существует ли соответствие. Сравнение/определение в блоке 130 и ромбовидной фигуре 140 может выполняться последовательно, до тех пор, пока не определится полная комбинация пароля, которая полностью соответствует сканированиям/перемещениям, сохраняемым в таблице. Далее управление переходит к ромбовидной фигуре 140, где может быть определено, соответствует ли последовательность отпечатка пальцев и направления таблице в базе данных. Если полное соответствие идентифицировано, то процесс идентификации был успешно завершён, и пользователь получил право доступа (ромбовидная фигура 150). В противном случае управление переходит к блоку 160, где в доступе может быть отказано. Следует заметить, что доступ может быть обеспечен к системе в целом, или к отдельному приложению, файлу и т.д. В то время как показанное в этом частном примере применения относится к варианту осуществления изобретения по фиг.4, объем настоящего изобретения не ограничивается в этом отношении.

Как обсуждалось выше, в других вариантах применения пользовательский ввод сканирования отпечатка пальца (с учетом направления или без него) может соответствовать символам, например алфавитно-цифровым символам клавиатуры. Соответственно, варианты осуществления изобретения для создания и аутентификации пароля, обсуждавшиеся выше в отношении фиг.3 и 4, могут быть изменены, чтобы включать в себя такие отображения соответствия. На фиг.5 другой вариант осуществления изобретения показывает способ для генерирования пароля в соответствии с вариантом осуществления настоящего изобретения. Как показано на фиг.5, способ 200 может быть использован для генерирования пароля. В целом способ действует таким же образом, как обсуждавшийся ранее и относящийся к фиг.3. В частности, может быть выполнена инициация фиксирования отпечатка пальца (блок 210). Затем может быть произведено сканирование отпечатка пальца с фиксированием направления метаданных или без него (блок 220). Затем это сканирование отпечатка пальца может быть отображено на соответствующий элемент пароля (блок 230). В одном варианте осуществления изобретения это отображение соответствия между элементом пароля (например, алфавитно-цифровым символом) и сканированием/направлением отпечатка пальца формирует ввод, который должен сохраняться в таблице базы данных, т.е. каждый введенный компонент таблицы может включать в себя соответствующее сканирование, символ и (возможно) направление сканирования. Выбрать элемент пароля может пользователь, или это может сделать компьютер. Затем управление переходит к ромбовидному элементу 240, где может быть определено, все ли пальцы были просканированы. Если нет, то управление переходит назад, к блоку 220, обсуждавшемуся выше.

Снова вернемся к фиг.5. Когда полное количество пальцев было просканировано, соответствия могут быть сохранены для пользователя в энергонезависимом запоминающем устройстве (блок 250). Например, может быть сохранена таблица, включающая в себя множество компонентов, каждый из которых соответствует данному сканированию (с использованием направления или без него), при этом могут сохраняться соответствующие отображения соответствия символам.

В одном варианте осуществления изобретения система может затем позволить пользователю выбрать пароль (блок 260) таким образом, что каждый палец (с

использованием направления или без него) отображает соответствие различному символу, являющемуся элементом пароля. В одном варианте осуществления изобретения это отображение соответствия может производиться через указатель расположения вводного компонента таблицы базы данных для пользователя для соответствующего символа, т.е. каждый вводимый компонент таблицы пароля может сохранять символ и указатель расположения таблицы базы данных для этого символа. Соответственно, этот пароль может ассоциироваться с отображением соответствия пользователя и может быть сохранен, например, в таблице пароля энергонезависимого запоминающего устройства (блок 270). В то время как показанное в этом частном примере применения относится к варианту осуществления изобретения по фиг.5, объем настоящего изобретения не ограничивается в этом отношении.

Аналогичным образом способ аутентификации может принимать во внимание такие отображения соответствия. На фиг.6 показана схема последовательности осуществления способа для аутентификации пароля в соответствии с другим вариантом осуществления настоящего изобретения. Как показано на фиг.6, способ 300 может начинаться таким образом, как обсуждалось выше в отношении фиг.4. В частности, множество отпечатков пальцев могут быть просканированы однократно (блок 310), при этом может быть определено, является ли действительным каждое такое изображение (ромбовидная фигура 320). Затем каждое упорядоченное изображение отпечатка пальца может сравниваться с базой данных таблиц (каждая из них служит для отдельного пользователя и включает в себя вводы для отображения соответствия сканирований/направлений и символов) и перемещает основанные на отображении данные на хранение в энергонезависимое запоминающее устройство (блок 330). Приведенные выше шаги могут быть выполнены для каждого вводного сканирования пользователя. Затем может быть определено, соответствуют ли перемещенные символы сохраняемому в памяти паролю для пользователя, представленному в базе данных пароля (ромбовидная фигура 340). Если нет, то может быть определено, соответствует ли количество предпринятых попыток получить доступ пороговому значению (ромбовидная фигура 380). Если нет, то отпечатки пальцев могут быть просканированы повторно. Если количество предпринятых попыток получить доступ равно пороговому значению, то управление переходит к блоку 390, когда доступ пользователя может быть отвергнут.

Если перемещенные символы соответствуют паролю, как определено в ромбовидной фигуре 340, далее может быть определено, соответствуют ли они стандартному паролю или паролю для состояния принуждения (ромбовидная фигура 350). То есть некоторые варианты осуществления изобретения могут позволять обнаружение альтернативного пароля, а именно пароля для состояния принуждения, который вводится в том случае, когда пользователь находится в состоянии принуждения, и может получить возможность минимального доступа к системе, и/или имеет возможность дать сигнал третьей стороне, чтобы предупредить о принуждении. В этих вариантах осуществления изобретения пользователь может ввести пароль с измененной комбинацией, находясь под принуждением, и система реагирует на этот пароль по-другому. Система может распознавать ввод как тревожный пароль и может дать ограниченный (или нет) доступ к системе, и/или может вызвать посылку сигнала тревоги о состоянии принуждения.

Если стандартный пароль соответствует необходимому при определении в ромбовидной фигуре 350, то управление переходит к блоку 370, где идентификация является успешной и пользователь получает доступ, т.е. нормальный пользователь имеет возможность получить доступ. Если вместо соответствия обнаруживается пароль для состояния принуждения, то управление может перейти к блоку 360, и в этом случае

успешная идентификация может привести к возможно ограниченному доступу для пользователя (или к отсутствию доступа) и инициации тревожного сигнала о принуждении.

5 Следует заметить, что способ по фиг.6 также может использоваться, чтобы принимать биометрический пользовательский ввод для пароля, сохраненного ранее как чисто алфавитно-цифровой пароль, позволяющий обратную совместимость, чтобы улучшить надежность. В то время как показанное в этом частном примере применения относится к вариантам осуществления изобретения по фиг.5 и 6, следует понимать, что объем настоящего изобретения не ограничивается в этом отношении, и, как обсуждалось 10 выше, сканирования отпечатков пальцев с направлениями перемещения или без них могут сами формировать пароль без перенесения или отображения на символы.

Множество видоизменений являются возможными. Например, в некоторых вариантах применения биометрическая аутентификация может использоваться как способ выполнения защищенного ввода (например, алфавитно-цифрового) символов, чтобы 15 ввести информацию, не являющуюся паролем, непосредственно в компьютер, без необходимости использовать клавиатуру. Таким образом, в публичном месте такая информация, как кредитная информация, может быть введена пользователем без набора ее на клавиатуре, тем самым позволяя обеспечить защищенный способ ввода информации.

20 По мере включения в пароль большого числа отдельных элементов степень аутентификации увеличивается. В некоторых вариантах применения может быть использовано различающееся количество элементов пароля, чтобы обеспечить изменяющиеся уровни доступа к системе или информации/приложениям в системе. Например, для разблокирования мобильного телефона, чтобы сделать телефонный 25 звонок, единственное скользящее перемещение единственного пальца может разблокировать его и позволить доступ к функции телефона. Однако для финансовой операции, когда требуется доступ к персональной информации (например, информации кредитной карточки), вместо использования только единственной цифры может потребоваться множество цифр/направлений (например, три пальца). Таким образом 30 могут быть реализованы градации аутентификации.

В одном примере единственная комбинация пароля может быть первым количеством элементов (например, 20). Различные части пароля (например, начиная от первого элемента) могут быть использованы для различных уровней аутентификации. Например, только один элемент может быть использован, чтобы получить доступ к устройству, 35 пять элементов используются для получения доступа к одному типу приложения, а остальные дополнительные элементы - для получения доступа к защищенным приложениям и т.д. Другие варианты осуществления изобретения могут позволять использовать пароль с N из M элементов. В таких вариантах применения аутентификация требует, по меньшей мере, N элементов из M элементов пароля, например три из десяти или три из пяти, и т.п. При использовании с одним вариантом осуществления изобретения N из M элементов могут применяться для задания размаха комбинации и количества 40 пальцев, которые должны быть использованы, при этом действительно используемые пальцы является несущественным фактором. Например, политика аутентификации может состоять в том, чтобы принимать, по меньшей мере, три различных пальца, каждый из которых имеет комбинацию перемещений. Другие варианты применения могут потребовать множество пальцев на обеих руках.

Существует множество паролей в повседневной жизни, и некоторые люди всегда забывают пароли, что вызывает большие неудобства. Используя вариант осуществления

изобретения, люди могли бы даже записывать свои пароли в ноутбук, не испытывая беспокойство за то, что они подвергаются риску, поскольку без физической комбинации пальцев и перемещений ввод одного пароля не позволит получить доступ.

5 Варианты осуществления изобретения могут быть включены в состав многих и различных обрабатывающих систем. Например, варианты осуществления изобретения могут быть использованы во взаимодействии с компьютерами в диапазоне от ноутбуков, настольных компьютеров и до служебных вычислительных машин, так же как и с мобильными сетевыми устройствами для работы с интернетом, смартфонами и т.п. Любая такая обрабатывающая система может включать в себя или взаимодействовать с биометрическим датчиком, который может быть сконфигурирован в системе или адаптирован к системе, например, как периферийное устройство, работающее через порт с универсальной последовательной шиной (USB). В некоторых вариантах применения более предпочтительной, чем специализированный биометрический датчик, является функция биометрического обнаружения, которая может быть реализована 10 через комбинацию сенсорного экрана (такого, как сенсорный экран с емкостным преобразованием) и программного обеспечения, программно-аппаратных средств и/или логики, чтобы преобразовывать действия на сенсорном экране в биометрические сканирования.

15 Фиг.7 является блок-схемой системы для использования с одним вариантом осуществления изобретения. В одном варианте осуществления изобретения обрабатывающая система 400 может быть мобильным сетевым устройством для работы с интернетом, таким как смартфон, хотя варианты осуществления изобретения могут быть объединены во множестве различных обрабатывающих систем. Как видно на фиг.7, система 400 включает в себя процессор 410 приложений, который может быть процессором общего назначения или специального назначения, таким как 25 микропроцессор, микроконтроллер, программируемая вентиляционная матрица (PGA - programmable gate array), или подобным устройством. Процессор 410 может включать в себя множество ядер 412 и кэш-память 414. Процессор 410 может дополнительно включать в себя контроллер 430 интегрированной памяти, который в одном варианте осуществления изобретения может быть присоединен к системной памяти 420 (например, динамическое ОЗУ, DRAM - dynamic random access memory). Процессор 410 может дополнительно включать в себя интегрированный контроллер - концентратор 440 ввода/вывода (I/O). Процессор 410 может быть присоединен к видеоконтроллеру 435, который, в свою очередь, может быть присоединен к дисплею 437, который может включать в себя сенсорный экран с емкостным преобразованием, чтобы принимать ввод от пользователя.

30 Флэш-память 460 может предусматривать энергонезависимое хранение данных, которые могут включать в себя таблицу пароля, включающую в себя вводы на биометрической основе для одного или более пользователей системы, и которые могут быть использованы для сравнения, чтобы принимать биометрические вводы от пользователя, предпринимая попытку получить доступ. Кроме того, процессор 450 немодулированной передачи может управлять средствами коммуникации через беспроводной интерфейс 462, который может быть использован для связи через сотовую или другие беспроводные сети.

45 Кроме того, биометрический датчик 470 может быть представлен в системе, чтобы позволить снятие отпечатков пальцев или другие виды сканирования, чтобы обеспечить безопасность для системы в соответствии с вариантом осуществления настоящего изобретения. В то время как датчик в варианте осуществления изобретения показан на

фиг.7 в виде отдельного компонента, следует понимать, что в других вариантах применения биометрический датчик 470 может быть сконфигурирован внутри дисплея. Хотя описание ссылается на специфические компоненты системы 400, предполагается, что многочисленные модификации и вариации описанных и проиллюстрированных вариантов осуществления изобретения также возможны.

Варианты осуществления изобретения могут быть применены в виде кода и могут сохраняться в запоминающем устройстве, имеющем хранящиеся в нем инструкции, которые могут быть использованы для программирования системы, чтобы выполнить эти инструкции. Запоминающее устройство может включать в себя, но не ограничиваясь этим, любой тип диска, включая гибкие диски, оптические диски, полупроводниковые диски (SSD, Solid State Disk), постоянные запоминающие устройства на компакт-диске (CD-ROM, Compact Disk Read Only Memory), перезаписываемые компакт-диски (CD-RW, Compact Disc Rewritable), магнитно-оптические диски, полупроводниковые устройства, такие как постоянное запоминающее устройство (ПЗУ, ROM), запоминающие устройства с произвольной выборкой (ЗУПВ, RAM, random-access memory), такие как динамическое ЗУПВ (DRAM, Dynamic Random-Access Memory), статическое ЗУПВ (SRAM, static random access memory), стираемое программируемое постоянное запоминающее устройство (СППЗУ, EPROM, Erasable Programmable Read-Only Memory), флэш-память, электрически стираемое программируемое постоянное запоминающее устройство (ЭСППЗУ, EEPROM, Erasable Electrically Programmable Read-Only Memory), магнитные или оптические карты, или любой другой тип носителя, подходящий для сохранения электронных инструкций.

В то время как описание настоящего изобретения относится к ограниченному количеству вариантов осуществления изобретения, специалисты в данной области техники будут принимать во внимание его многочисленные модификации и вариации. Предполагается, что прилагаемая формула изобретения покрывает все такие модификации и вариации, которые попадают в пределы действительного объема и сущности настоящего изобретения.

Формула изобретения

1. Способ доступа к обрабатывающей системе, содержащий этапы, на которых: принимают упорядоченную последовательность вводов биометрических данных от пользователя через биометрический датчик, связанный с обрабатывающей системой; определяют наличие совпадения каждого из вводов биометрических данных упорядоченной последовательности с соответствующей записью, хранящейся в таблице энергонезависимого запоминающего устройства обрабатывающей системы, при этом таблица включает в себя сохраненную упорядоченную последовательность вводов биометрических данных, соответствующую комбинации пароля пользователя; и при наличии совпадения предоставляют пользователю доступ к обрабатывающей системе, а при отсутствии совпадения не допускают доступ пользователя к обрабатывающей системе, при этом каждый из вводов биометрических данных упорядоченной последовательности соответствует различному пальцу пользователя и соответствует элементу комбинации для пароля, выбранной пользователем, причем первый палец пользователя соответствует первому алфавитно-цифровому символу, выбранному пользователем, а второй палец пользователя соответствует второму алфавитно-цифровому символу, выбранному пользователем.

2. Способ по п.1, в котором каждый из вводов биометрических данных упорядоченной последовательности соответствует различному пальцу пользователя и направлению

перемещения пальца на биометрическом датчике.

3. Способ по п.1, в котором каждая запись дополнительно содержит отображение, устанавливающее соответствие между одним из вводов биометрических данных сохраняемой упорядоченной последовательности и алфавитно-цифровым символом.

5 4. Способ по п.3, дополнительно содержащий этап, на котором, если каждый из вводов биометрических данных совпадает с соответствующей записью, определяют, совпадает ли совокупность алфавитно-цифровых символов каждой записи сохраненному паролю в базе данных паролей.

10 5. Способ по п.1, дополнительно содержащий этап, на котором предоставляют пользователю доступ к ограниченному участку обрабатывающей системы, когда число вводов биометрических данных упорядоченной последовательности меньше числа вводов биометрических данных хранящейся в памяти упорядоченной последовательности.

15 6. Способ по п.1, в котором упорядоченная последовательность вводов биометрических данных имеет первую длину N , а хранящаяся в памяти упорядоченная последовательность вводов биометрических данных имеет вторую длину M , при этом N меньше M .

20 7. Способ по п.1, дополнительно содержащий этап, на котором предоставляют пользователю доступ к первой функции обрабатывающей системы в ответ на единственный ввод биометрических данных, совпадающий с первым из вводов биометрических данных хранящейся в памяти упорядоченной последовательности.

8. Способ по п.7, в котором первая функция является функцией телефона обрабатывающей системы.

25 9. Способ по п.8, дополнительно содержащий этап, на котором предоставляют пользователю доступ ко второй функции обрабатывающей системы в ответ на множество вводов биометрических данных, совпадающих с соответствующим множеством вводов биометрических данных хранящейся в памяти упорядоченной последовательности.

30 10. Способ по п.9, в котором вторая функция позволяет пользователю выполнять защищенную финансовую операцию, включающую в себя информацию о счете пользователя.

11. Доступный для машины носитель данных, содержащий команды, которые при их исполнении вызывают выполнение системой:

35 запроса пользователю ввести упорядоченную последовательность вводов биометрических данных через биометрический датчик, связанный с системой, при этом каждый ввод биометрических данных упорядоченной последовательности обеспечивает направление перемещения пальца относительно биометрического датчика;

приема упорядоченной последовательности вводов биометрических данных в систему от пользователя через биометрический датчик; и

40 сохранения результата сканирования каждого ввода биометрических данных упорядоченной последовательности, метаданных, относящихся к направлению перемещения, и алфавитно-цифрового символа в записи в таблице, связанной с пользователем, причем таблица хранится в энергонезависимом запоминающем устройстве, при этом каждый из вводов биометрических данных упорядоченной последовательности содержит алфавитно-цифровой символ, выбранный пользователем для соответствия указанному биометрическому вводу.

12. Доступный для машины носитель данных по п.11, дополнительно содержащий команды, которые при их исполнении вызывают предоставление системой пользователю

возможности выбрать пароль.

13. Доступный для машины носитель данных по п.12, дополнительно содержащий команды, которые при их исполнении вызывают сохранение системой соответствия пароля записям в таблице, при этом соответствие для элемента пароля содержит указатель на запись в таблице, включающую в себя алфавитно-цифровой символ элемента.

14. Доступный для машины носитель данных по п.11, дополнительно содержащий команды, которые при их исполнении вызывают выполнение системой:

приема второй упорядоченной последовательности вводов биометрических данных в систему от пользователя через биометрический датчик; и

определения наличия совпадения каждого из вводов биометрических данных второй упорядоченной последовательности с соответствующей записью, хранящейся в таблице, и при положительном результате определения предоставления пользователю доступа к системе, а в противном случае недопущения доступа пользователя к системе.

15. Доступный для машины носитель данных по п.14, дополнительно содержащий команды, которые при их исполнении вызывают определение системой соответствия второй упорядоченной последовательности вводов биометрических данных паролю для состояния принуждения и при положительном результате определения передачи тревожного сигнала о состоянии принуждения третьей стороне.

16. Доступный для машины носитель данных по п.14, дополнительно содержащий команды, которые при их исполнении вызывают определение системой совпадения каждого из вводов биометрических данных второй упорядоченной последовательности с записью в таблице, при этом число вводов биометрических данных второй упорядоченной последовательности меньше числа вводов биометрических данных упорядоченной последовательности.

17. Обработывающая система для осуществления доступа, содержащая:

процессор для исполнения команд для приема упорядоченной последовательности вводов биометрических данных от пользователя, определения наличия совпадения каждого из вводов биометрических данных упорядоченной последовательности с соответствующей записью, хранящейся в таблице, включающей в себя сохраненную упорядоченную последовательность вводов биометрических данных, соответствующую комбинации пароля для пользователя, и при положительном результате определения предоставления пользователю доступа к системе, а в противном случае недопущения доступа пользователя к системе;

биометрический датчик, связанный с процессором, для подачи упорядоченной последовательности вводов биометрических данных в процессор; и

энергонезависимое запоминающее устройство, связанное с процессором, для хранения таблицы,

при этом каждая запись в таблице дополнительно содержит отображение, связывающее один из вводов биометрических данных сохраненной упорядоченной последовательности с алфавитно-цифровым символом, причем первый палец пользователя соответствует первому алфавитно-цифровому символу, выбранному пользователем, а второй палец пользователя соответствует второму алфавитно-цифровому символу, выбранному пользователем.

18. Система по п.17, в которой каждая запись в таблице дополнительно содержит отображение, связывающее один из вводов биометрических данных сохраненной упорядоченной последовательности с направлением перемещения соответствующего ввода биометрических данных.

19. Система по п.17, в которой энергонезависимое запоминающее устройство дополнительно содержит базу данных пароля для хранения множества записей, каждая из которых соответствует паролю для пользователя.

5 20. Система по п.19, в которой каждая запись базы данных пароля содержит отображение пароля на записи таблицы, при этом отображение для элемента пароля содержит указатель на запись в таблице, включающую в себя алфавитно-цифровой символ элемента пароля.

10

15

20

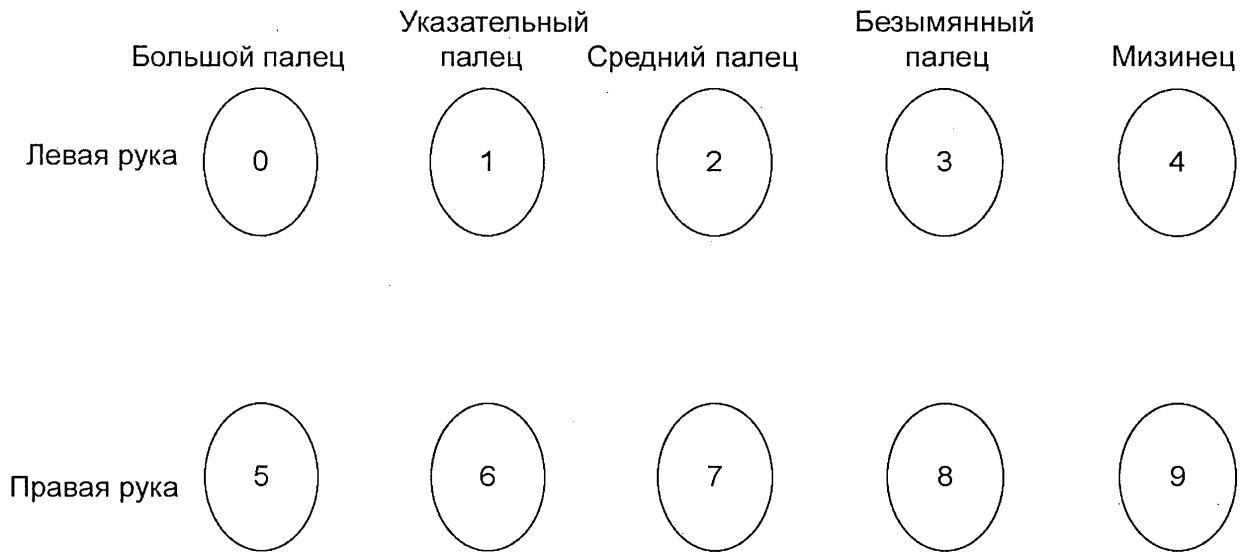
25

30

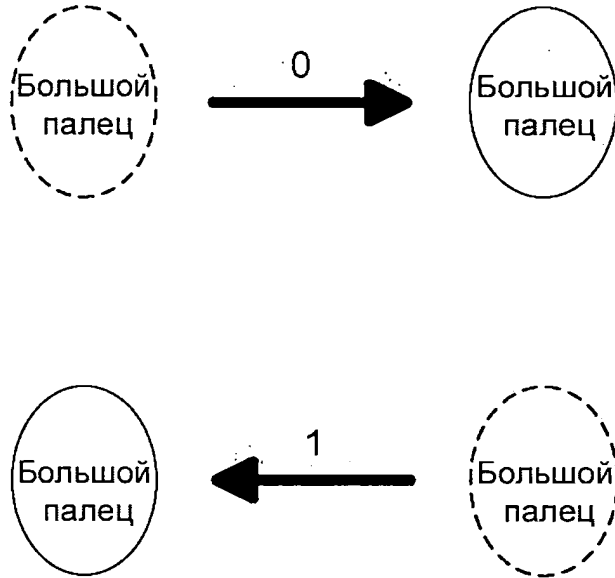
35

40

45



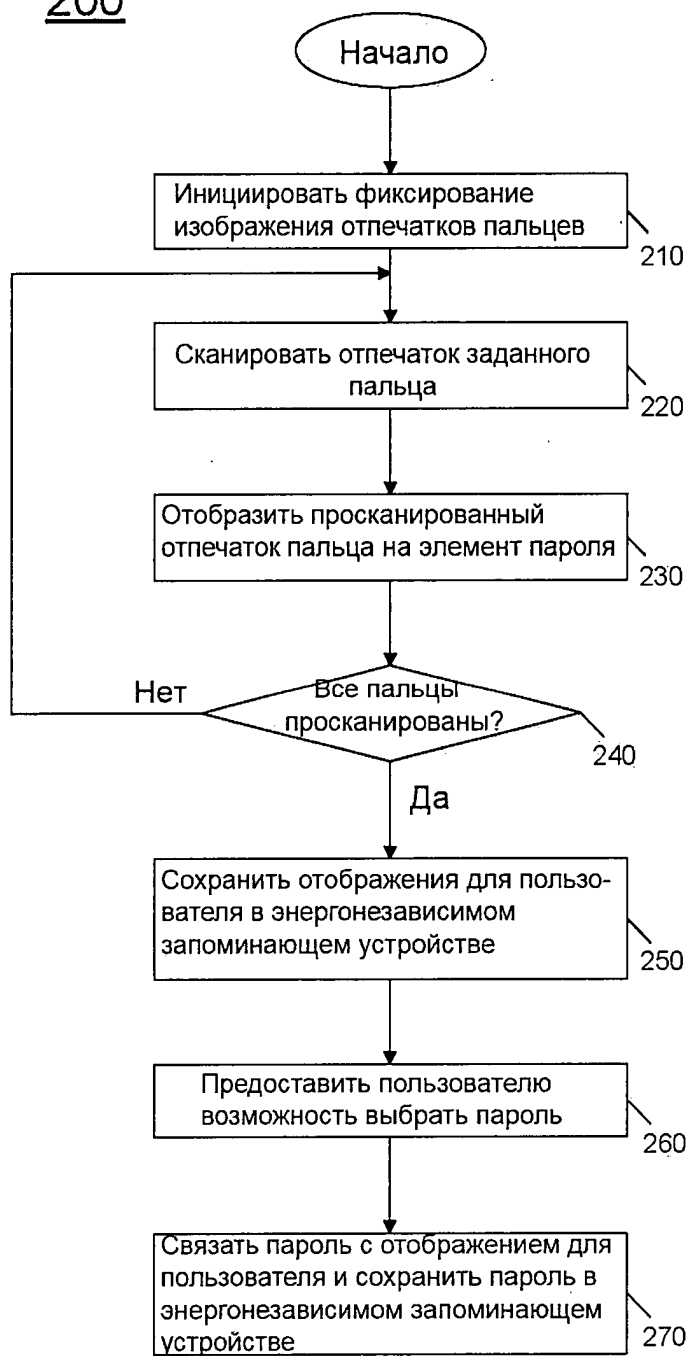
Фиг. 1



Фиг. 2

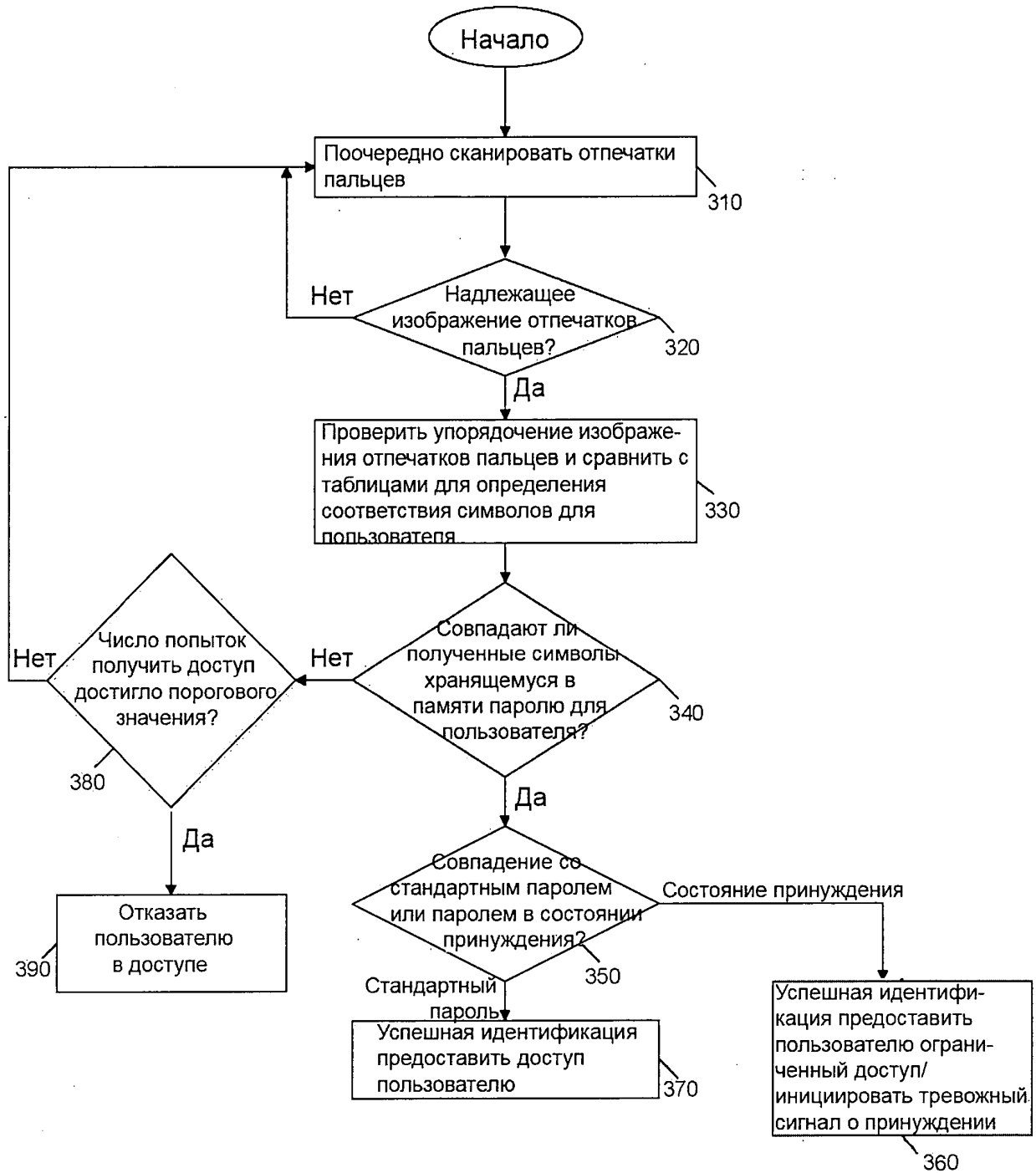
10

Фиг. 3

200

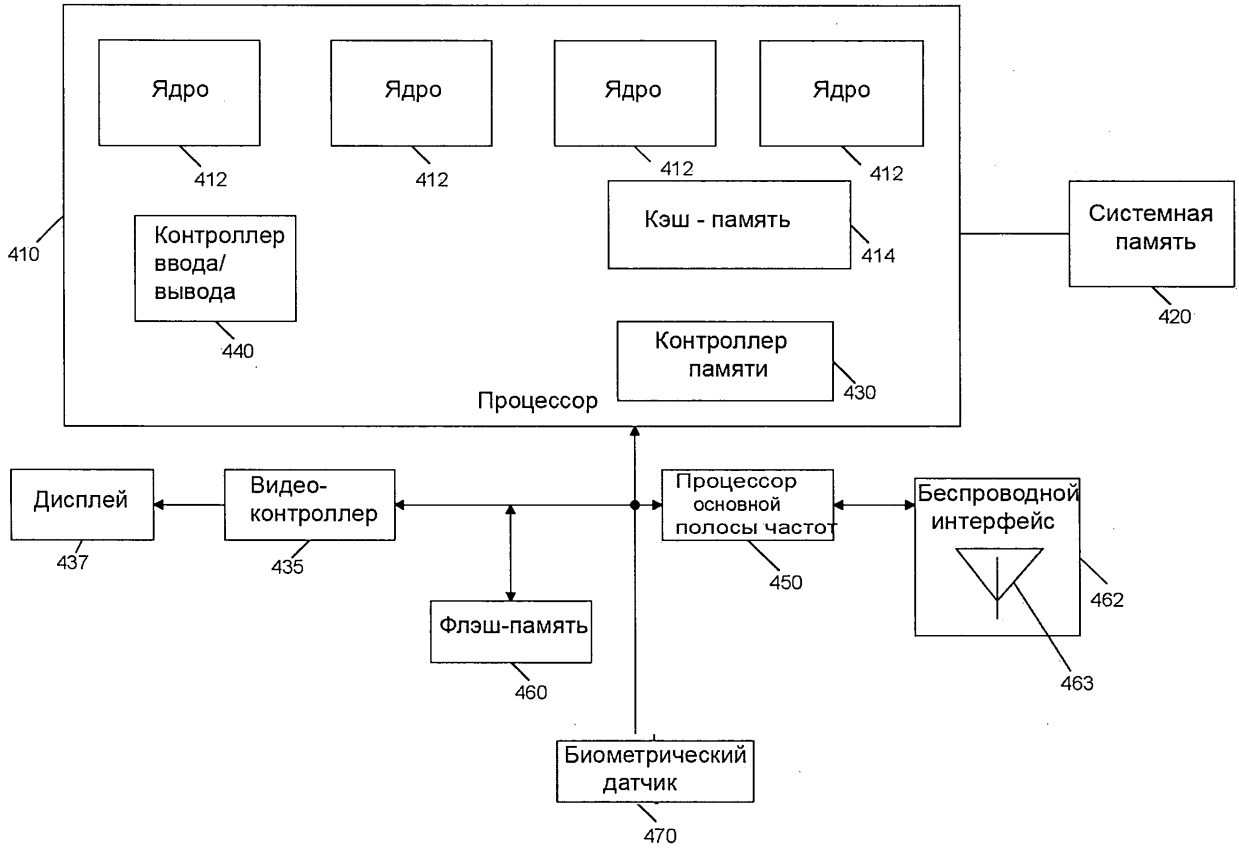
Фиг. 5

300



ФИГ. 6

400



Фиг. 7