(19) Евразийское патентное ведомство

(11) 045306 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.11.15

(21) Номер заявки
202390227

(22) Дата подачи заявки
2022.12.30

(51) Int. Cl. *G06F 21/36* (2013.01)

(54) СПОСОБ ПРОВЕДЕНИЯ АУТЕНТИФИКАЦИИ

(31) **2022127829**
(32) **2022.10.26**
(33) **RU**
(43) **2023.11.14**
(96) **2022000149 (RU) 2022.12.30**

(71)(73) Заявитель и патентовладелец:
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "КАПЧА СОЛЮШНЗ" (RU)

(72) Изобретатель:
Анисимов Андрей Александрович (RU)

(74) Представитель:
Котлов Д.В. (RU)

(56) RU-C1-2768567
RU-C1-2728505
US-20130347087
CN-A-109918883
CN-A-107679391

(57) Изобретение относится к области компьютерной техники, а именно к способам проведения аутентификации пользователей с помощью графических изображений, и может быть использовано, например, в качестве теста CAPTCHA для различения компьютеров и людей или для разблокирования персональных устройств, оборудования, дверей и т.д. Способ проведения аутентификации включает следующие этапы: (i) формируют шаблоны графических изображений, (ii) демонстрируют один из указанных шаблонов пользователю и предлагают пользователю изобразить продемонстрированный шаблон, (iii) регистрируют набор ключевых параметров сформированного пользователем изображения, (iv) сравнивают набор ключевых параметров сформированного пользователем изображения с соответствующим набором ключевых параметров шаблона и выдают сигнал успешной аутентификации, если их разница не выходит за пределы доверительного диапазона. В указанный набор ключевых параметров включают, по меньшей мере, один временной параметр, характеризующий динамику появления траектории, по которой пользователем было сформировано изображение. На этапе (i) для каждого шаблона указанный набор ключевых параметров и пределы доверительного диапазона определяют методом машинного обучения на основе тестовых изображений, которые были вручную сформированы ранее аутентифицированными пользователями при демонстрации этого шаблона. Изобретение позволяет значительно повысить надёжность проведения аутентификации.

045306 B1

045306 B1

Область техники

Изобретение относится к области компьютерной техники, а именно, к способам проведения аутентификации пользователей с помощью графических изображений и может быть использовано, например, в качестве теста CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart - полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей) или для разблокирования персональных устройств, оборудования, дверей и т.д.

Уровень техники

С момента широкого распространения сайтов их владельцы стали сталкиваться с различными видами мошенничества и спама из-за использования компьютерных ботов (роботов) злоумышленниками. В 2000-2001 годах для решения этой проблемы на сайты стали устанавливать защиту на страницы регистрации с помощью CAPTCHA: пользователей просили перепечатать искаженный текст, который программы с трудом распознают (см. Stringham, Edward P (2015). Private Governance: creating order in economic and social life. Oxford University Press. p. 105. ISBN 978-0-19-936516-6. OCLC 5881934034). По данным компании Datanyze технология распознавания пользователя от робота по типу CAPTCHA установлена на более чем 3500000 доменах в сети Интернет. Более 50 миллиардов раз в месяц пользователи решают капчи. Хотя этот механизм обеспечивает хорошую безопасность и ограничивает автоматическую регистрацию веб-службами, некоторые CAPTCHA имеют ряд недостатков, которые позволяют ботам проходить проверку как человек. В связи с этим исследуется возможность применения широко распространённых сегодня биометрических технологий для решения указанной задачи и разработки специализированного программного обеспечения.

Из уровня техники известен способ реализации теста CAPTCHA, который основан на демонстрации пользователю простых текстовых символов с зашумлением и определении воспроизведения этих символов пользователем с использованием известных алгоритмов метрики близости (см. патент US 8978144 B2, кл. G06F 21/30, опубл. 10.03.2015). Для дополнительной защиты от повторения ботами в известном способе при демонстрации добавляют динамические эффекты (показывают буквы поочередно, удаляют частички случайным образом и т.п.). Основными недостатками известного способа являются сложность реализации и недостаточная достоверность теста, обусловленная относительной простотой компьютерного взлома демонстрируемых изображений.

Из уровня техники известен способ реализации теста CAPTCHA, согласно которому демонстрируют пользователю шаблон графического изображения и предлагают обозначить это изображение одним или несколькими понятиями, при этом аутентификацию проводят с использованием зарегистрированного времени решения теста пользователем (см. патент US 8752141 B2, кл. G06F 7/04, опубл. 10.06.2014). Основными недостатками известного способа являются неудобство его использования и недостаточная достоверность, обусловленная относительной простотой компьютерного взлома посредством современных алгоритмов распознавания образов.

Из уровня техники известен способ аутентификации пользователя, согласно которому регистрируют декартовы координаты точек линии, проводимой пользователем в процессе рисования изображения, и время рисования, после чего сравнивают набор ключевых параметров сформированного изображения с соответствующим набором ключевых параметров эталонного изображения, заранее созданного аутентифицированным пользователем (см. патент US 11238149 B2, кл. G06F 21/31, опубл. 01.02.2022). Известный способ может быть использован в системе разблокирования портативных вычислительных устройств. Основным недостатком известного способа является недостаточная надёжность различения компьютеров и людей.

Из уровня техники известен способ проведения аутентификации, согласно которому формируют шаблон графического изображения путём объединения нескольких заранее заданных элементов, демонстрируют его пользователю, регистрируют набор координат сформированного пользователем изображения, выделяют достаточное количество точек для сравнения, сравнивают их с соответствующим набором координат шаблона и выдают сигнал успешной аутентификации, если их разница не выходит за пределы доверительного диапазона (см. патент US 9471767 B2, кл. G06F 21/36, опубл. 18.10.2016). Недостатком известного способа является то, что оценивается только насколько далеко точки нарисованной и демонстрируемой траектории располагаются друг от друга, а в части динамики рисования учитывается только, что время генерации изображения ботами больше, чем время рисования для человека. Таким образом, основным недостатком известного способа являются ограниченные возможности, обусловленные малым количеством регистрируемых данных, что значительно упрощает взлом системы аутентификации, работающей по такому способу.

Наиболее близким по технической сущности к предлагаемому изобретению является способ проведения аутентификации, согласно которому реализуют следующие этапы: формируют шаблоны графических изображений, демонстрируют один из указанных шаблонов пользователю, предлагают пользователю изобразить продемонстрированный шаблон, регистрируют набор ключевых параметров сформированного пользователем изображения, сравнивают набор ключевых параметров сформированного пользователем изображения с соответствующим набором ключевых параметров шаблона и выдают сигнал успешной аутентификации, если их разница не выходит за пределы доверительного диапазона (см. патент

US 10657243 B2, кл. G06F 21/36, опубл. 19.05.2020). В качестве шаблона изображения используют случайно сгенерированную эталонную траекторию, а в ходе сравнения определяют, каким образом характерные (опорные) точки располагаются друг от друга на траектории. Недостатком известного способа является относительно высокая вероятность взлома, поскольку успешная аутентификация определяется только тем, какой объект и за какое суммарное время был нарисован.

Сущность изобретения

Технической проблемой является устранение вышеуказанных недостатков.

Технический результат заключается в повышении надёжности проведения аутентификации. Поставленная задача решается, а технический результат достигается тем, что способ проведения аутентификации включает следующие этапы: (i) формируют шаблоны графических изображений, (ii) демонстрируют один из указанных шаблонов пользователю и предлагают пользователю изобразить продемонстрированный шаблон, (iii) регистрируют набор ключевых параметров сформированного пользователем изображения, (iv) сравнивают набор ключевых параметров сформированного пользователем изображения с соответствующим набором ключевых параметров шаблона и выдают сигнал успешной аутентификации, если их разница не выходит за пределы доверительного диапазона, причём в указанный набор ключевых параметров включают, по меньшей мере, один временной параметр, характеризующий динамику появления траектории, по которой пользователем было сформировано изображение, а на этапе (i) для каждого шаблона указанный набор ключевых параметров и пределы доверительного диапазона определяют методом машинного обучения на основе тестовых изображений, которые были вручную сформированы ранее аутентифицированными пользователями при демонстрации этого шаблона. Указанный временной параметр может представлять собой среднюю скорость на траектории, проекцию ускорения на начальную часть траектории, среднее количество точек на траектории за выбранные интервалы времени, интервалы времени, за которые пользователем были сформированы выбранные части изображения, среднее и/или среднеквадратическое отклонение длины интервалов времени между выбранными точкам траектории. Указанный набор ключевых параметров может дополнительно включать площадь под траекторией в проекции на выбранную ось координат и длину траектории. В указанные пределы доверительного диапазона могут включать верхнее пороговое значение и нижнее пороговое значение, а сигнал успешной аутентификации на этапе (iv) выдавать, если указанная разница ключевых параметров сформированного пользователем изображения и шаблона находится между указанными верхним пороговым значением и нижним пороговым значением. На этапе (ii) шаблон предпочтительно демонстрируют с зашумлением и/или в виде анимации. Сигнал успешной аутентификации предпочтительно используют как сигнал прохождения теста CAPTCHA или как сигнал разблокирования.

Описание чертежей

На фиг. 1 представлен скриншот перед началом этапа (ii) демонстрации шаблона графического изображения;

на фиг. 2 представлен скриншот этапа (ii) демонстрации шаблона графического изображения на экране мобильного телефона;

на фиг. 3 представлен скриншот этапа (ii) демонстрации шаблона графического изображения на экране планшета или персонального компьютера;

на фиг. 4 - блок-схема алгоритма демонстрирования шаблона графического изображения с зашумлением, показа пользователю и обработки данных;

на фиг. 5 - блок-схема алгоритма проведения аутентификации согласно предлагаемому способу.

Детальное описание изобретения

В качестве альтернативы существующим вариантам CAPTCHA согласно предлагаемому способу пользователю предлагается повторить шаблон графического изображения в виде фигуры-рисунка, а собираемые сведения при построении изображения будут использованы для аутентификации. Предлагаемое изобретение основано на том, что наиболее сложными с точки зрения имитации (спуфинга) с целью взлома для обеспечения несанкционированного доступа является воссоздание поведенческих особенностей, в частности, манеры рисования (биометрического почерка). Основным преимуществом биометрии является её уникальность и многопараметричность, поэтому параметры, связанные с человеческой деятельностью, практически невозможно повторить или подделать. В предложенном изобретении предлагается в ходе аутентификации использовать не только векторизованные характеристики сформированного изображения, но и векторизованные характеристики самого процесса рисования изображения, полученные за счет использования сверточных глубоких нейронных сетей (такие сети могут предварительно обучаться на огромном объеме любых изображений и далее дообучаться на пополняемой базе данных).

Предлагаемый способ проведения аутентификации включает следующие основные этапы.

Этап (i) формирования шаблонов графических изображений.

Исходные шаблоны графических изображений могут быть загружены в систему аутентификации из внешнего источника или предложены ранее аутентифицированными пользователями и предпочтительно представляют собой простые монохромные объекты (рисунки). Для каждого шаблона методом машинного обучения на основе тестовых изображений формируют набор ключевых параметров, который прикрепляют к указанному шаблону. В качестве тестовых изображений используют изображения, которые бы-

ли вручную сформированы ранее аутентифицированными пользователями при демонстрации этого шаблона. Для сбора детерминированных данных, могут быть использованы как открытые площадки, так и пользователи платформы Яндекс. Толока.

Пополнение базы данных может осуществляться как готовыми изображениям, так и теми, которые предлагают новые пользователи, а также за счет автоматической генерацией шаблона с дальнейшим переобучением нейронной сети после его показа реальным пользователям и сбора информации о наборе ключевых параметров.

Для обеспечения максимальной надёжности предлагаемого способа аутентификации в набор ключевых параметров включают, по меньшей мере, один временной параметр, характеризующий динамику появления траектории, по которой пользователем было сформировано изображение (т.е. манеру рисования).

Указанный временной параметр может представлять собой:

среднюю скорость на траектории;

мгновенную скорость по осям X, Y в каждой точке траектории;

проекцию ускорения на начальную часть траектории (например, на первые 10 точек);

среднее количество точек на траектории за выбранные интервалы времени;

интервалы времени, за которые пользователем были сформированы выбранные части изображения (например, отдельные четверти рисунка);

среднее и/или среднеквадратическое отклонение длины интервалов времени между выбранными (характерными) точкам траектории;

отношение скоростей/ускорений/времени формирования последующего отрезка к предыдущему;

отношение отрезка скорости/ускорения/времени к общему значению и т.п.

Дополнительно набор ключевых параметров может включать нединамические параметры, такие как площадь под траекторией в проекции на оси X, Y координат;

общую длину траектории;

кратчайшее расстояние между характерными точками траектории и его отношение ко всей длине траектории;

углы наклона к осям X и Y прямой между началом и концом первой четверти траектории и т.п.

Благодаря используемым алгоритмам глубокого обучения нейронных сетей на этом этапе могут быть определены основные характерные особенности, присущие манере рисования предложенного изображения человеком, которые на современном уровне развития техники практически невозможно подделать программно.

Характеристики объектов сохраняются в векторизованном виде (на входе сложно структурированные "сырые" данные объектов, а на выходе векторные представления характеристики в виде набора ключевых параметров). Данные вектора получаются способом прогона входных данных через предварительно обученную глубокую нейронную сеть (ПОГНС) с использованием технологии Deep Learning (глубокое машинное обучение). ПОГНС изначально обучается человеком путем ручной разметки заранее собранных объектов в похожие классы, после чего ПОГНС сохраняется для непосредственной векторизации входных данных.

Аналогичным образом с помощью машинного обучения определяют пределы доверительного диапазона. Указанные пределы доверительного диапазона могут включать как верхнее пороговое значение (когда параметры сформированного изображения слишком далеки от шаблона - например, более 30% различия), так и нижнее пороговое значение (когда параметры сформированного изображения, наоборот, слишком похожи на шаблон и вероятно были скопированы посредством компьютерного взлома - например, менее 3% различия).

Дополнительно могут быть проанализированы данные об устройстве пользователя, его интернет-идентификаторы (IP-адрес и пр.) на сопоставление с возможным использованием роботом (использование дополнительных открытых и коммерческих баз).

Этап (ii) демонстрации одного из указанных шаблонов пользователю.

На этом этапе выбирают один из имеющихся шаблонов и демонстрируют его на экране устройства пользователю (см. фиг. 1, 2, 3). Для снижения вероятности взлома шаблон демонстрируют с зашумлением, т.е. наложением случайных шумов (см. фиг. 4), а для упрощения последующего анализа - в виде анимации, показывающей, по какой траектории следует рисовать предложенный шаблон. По завершении этого этапа предлагают пользователю изобразить (повторить) продемонстрированный шаблон с помощью сенсорного экрана мобильного устройства, ноутбука (тачпад) или компьютерной мыши.

Этап (iii) регистрации набора ключевых параметров сформированного пользователем изображения.

В ходе формирования изображения пользователем система в динамике регистрирует процесс появления траектории (координаты точек на сенсорном экране и астрономическое или относительное время их появления), по которой пользователь рисует изображение, и передаёт полученные данные на удалённый сервер для последующей обработки и выявления значений ключевых параметров.

Этап (iv) сравнения и завершения аутентификации.

На этом этапе набор ключевых параметров сформированного пользователем изображения сравни-

вают с соответствующим набором ключевых параметров шаблона. Предпочтительным вариантом является использование в качестве метрики близости между наборами ключевых параметров (векторами) косинусного расстояния.

Сигнал успешной аутентификации выдают, если разница этих параметров не выходит за пределы доверительного диапазона (т.е. находится между верхним и нижним пороговыми значениями). В противном случае процедуру повторяют или выдают уведомление об ошибке в соответствии с алгоритмом на фиг. 4.

Сигнал успешной аутентификации можно использовать как сигнал прохождения теста CAPTCHA (например, для обеспечения доступа на сайт) или как сигнал разблокирования персональных устройств, оборудования, дверей и т.п. (см. фиг. 5).

За счёт использования в качестве основы распознавания особенностей биометрического почерка, предложенный способ позволяет значительно повысить надёжность аутентификации как при применении в качестве теста CAPTCHA, так и при применении в качестве ключа разблокировки.

Опробование предлагаемого способа было проведено с использованием алгоритма глубокого машинного обучения по типу нейронной сети с более, чем 300 слоев и 1 миллиона параметров. Всего в ходе опробования собрано более 21000 биометрических образцов. В среднем каждым пользователем выполнено повторение 30 фигур из набора более 700 фигур и сформированы образцы биометрических почерков для каждого изображения с координатно-временным характеристиками для обучения глубоких нейронных сетей. Датасеты собирались с использованием JavaScript в виде изображений рисунков, а также перечня координат X, Y и времени каждые несколько миллисекунд.

В результате опробования способа были получены следующие параметры системы идентификации:

время на аутентификацию в среднем составило порядка 6 секунд;

более 90 % пользователей смогли понять и пройти аутентификацию с первого раза;

точность распознавания ботов и пользователей составила более 90%.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ проведения аутентификации, согласно которому реализуют следующие этапы,

(i) формируют шаблоны графических изображений,

(ii) демонстрируют один из указанных шаблонов пользователю и предлагают пользователю изобразить продемонстрированный шаблон,

(iii) регистрируют набор ключевых параметров сформированного пользователем изображения,

(iv) сравнивают набор ключевых параметров сформированного пользователем изображения с соответствующим набором ключевых параметров шаблона и выдают сигнал успешной аутентификации, если их разница не выходит за пределы доверительного диапазона,

отличающийся тем, что

в указанный набор ключевых параметров включают, по меньшей мере, один временной параметр, характеризующий динамику появления траектории, по которой пользователем было сформировано изображение, а

на этапе (i) для каждого шаблона указанный набор ключевых параметров и пределы доверительного диапазона определяют методом машинного обучения на основе тестовых изображений, которые были вручную сформированы ранее аутентифицированными пользователями при демонстрации этого шаблона.

2. Способ по п.1, отличающийся тем, что указанный временной параметр представляет собой среднюю скорость на траектории.

3. Способ по п.1, отличающийся тем, что указанный временной параметр представляет собой проекцию ускорения на выбранную ось координат.

4. Способ по п.1, отличающийся тем, что указанный временной параметр представляет собой среднее количество точек на траектории за выбранные интервалы времени.

5. Способ по п.1, отличающийся тем, что указанный временной параметр представляет собой интервалы времени, за которые пользователем были сформированы выбранные части изображения.

6. Способ по п.1, отличающийся тем, что указанный временной параметр представляет собой среднее и/или среднеквадратическое отклонение длины интервалов времени между выбранными точкам траектории.

7. Способ по п.1, отличающийся тем, что указанный набор ключевых параметров включает площадь под траекторией в проекции на выбранную ось координат.

8. Способ по п.1, отличающийся тем, что указанный набор ключевых параметров включает длину траектории.

9. Способ по п.1, отличающийся тем, что указанные пределы доверительного диапазона включают верхнее пороговое значение и нижнее пороговое значение, а сигнал успешной аутентификации на этапе (iv) выдают, если указанная разница ключевых параметров сформированного пользователем изображения и шаблона находится между указанными верхним пороговым значением и нижним пороговым зна-

чением.

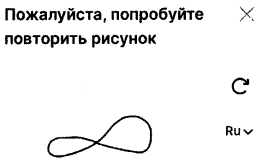
10. Способ по п.1, отличающийся тем, что на этапе (ii) шаблон демонстрируют с зашумлением.

11. Способ по п.1, отличающийся тем, что на этапе (ii) шаблон демонстрируют в виде анимации.

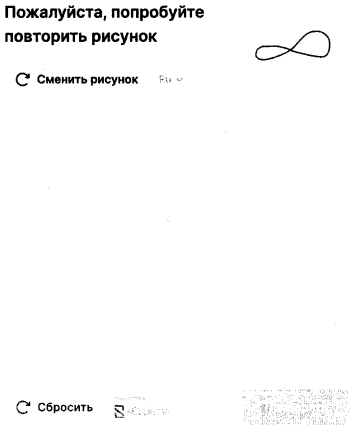
12. Способ по п.1, отличающийся тем, что сигнал успешной аутентификации используют как сигнал прохождения теста CAPTCHA.

13. Способ по п.1, отличающийся тем, что сигнал успешной аутентификации используют как сигнал разблокирования.

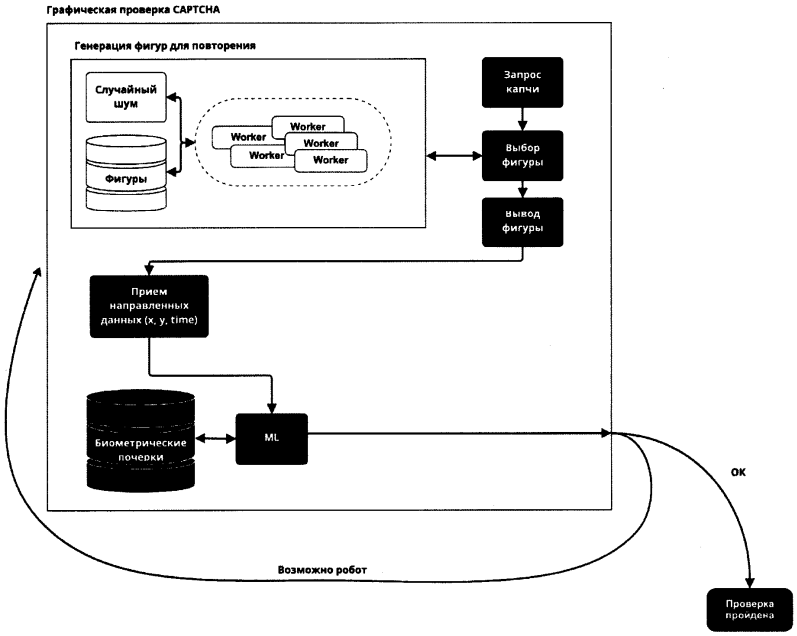
Фиг. 1



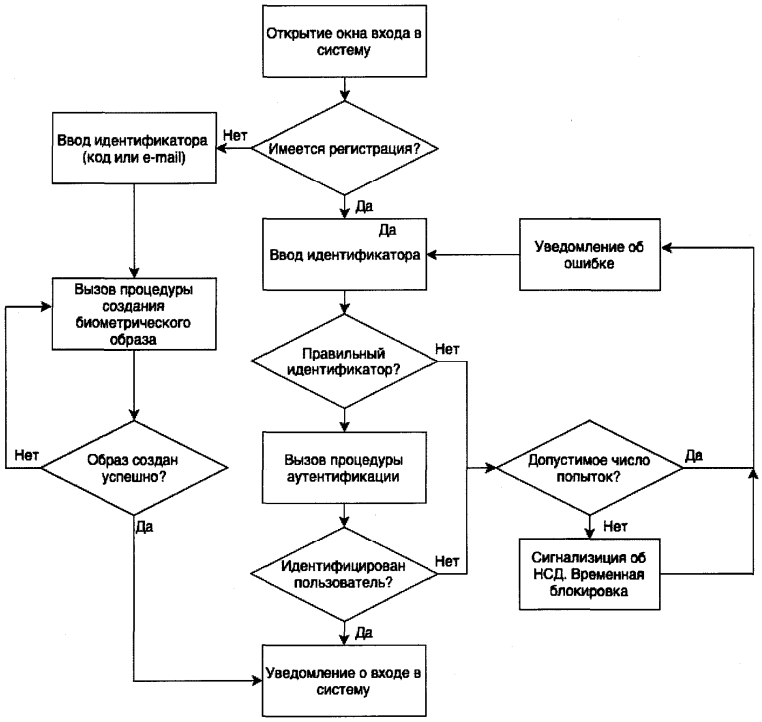
Фиг. 2



Фиг. 3


Графическая проверка CAPTCHA
Генерация фигур для повторения
Случайный шум
Фигуры
Worker
Worker
Worker
Worker
Worker
Запрос капчи
Выбор фигуры
Вывод фигуры
Прием направленных данных (x, y, time)
Биометрические почерки
ML
ok
Возможно робот
Проверка пройдена

Фиг. 4


Открытие окна входа в систему
Имеется регистрация?
Нет
Ввод идентификатора (код или e-mail)
Да
Ввод идентификатора
Да
Уведомление об ошибке
Вызов процедуры создания биометрического образа
Правильный идентификатор?
Нет
Образ создан успешно?
Нет
Да
Вызов процедуры аутентификации
Допустимое число попыток?
Да
Нет
Идентифицирован пользователь?
Нет
Сигнализация об НСД. Временная блокировка
Да
Уведомление о входе в систему

Фиг. 5