



(51) МПК
G10L 17/14 (2013.01)
G10L 17/24 (2013.01)
G10L 15/00 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
 ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2013136376/08, 05.08.2013

(24) Дата начала отсчета срока действия патента:
 05.08.2013

Приоритет(ы):

(22) Дата подачи заявки: 05.08.2013

(43) Дата публикации заявки: 10.02.2015 Бюл. № 4

(45) Опубликовано: 20.09.2016 Бюл. № 26

(56) Список документов, цитированных в отчете о поиске: US 2011/0276323 A1, 10.11.2011; US 2006/0111898 A1, 25.05.2006; US 2004/0234137 A1, 25.11.2004; US 6957185 B1, 18.10.2005. RU 2419890 C1, 27.05.2011.

Адрес для переписки:

197227, Санкт-Петербург, а/я 405, Воропаю
 Сергею Александровичу

(72) Автор(ы):

Хитров Михаил Васильевич (RU),
 Дырмовский Дмитрий Викторович (RU)

(73) Патентообладатель(и):

Общество с ограниченной ответственностью
 "Центр речевых технологий" (ООО "ЦРТ")
 (RU)

(54) СПОСОБ ОЦЕНКИ ВАРИАТИВНОСТИ ПАРОЛЬНОЙ ФРАЗЫ (ВАРИАНТЫ)

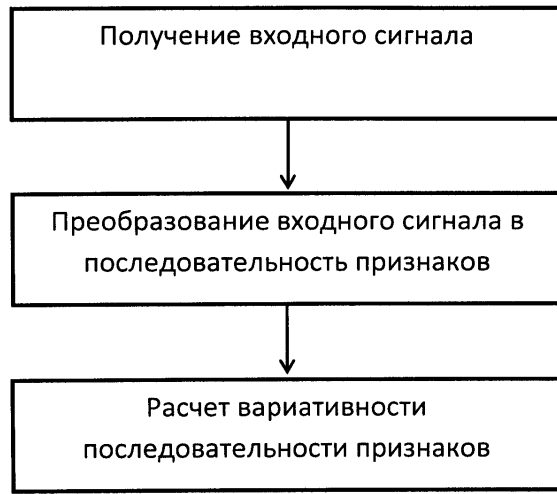
(57) Реферат:

Изобретение относится к области распознавания речи. Технический результат - обеспечение надежной оценки вариативности парольных фраз. Способ оценки вариативности парольной фразы, включающий получение парольной фразы от пользователя и оценку ее вариативности, отличающийся тем, что получают от пользователя парольную фразу в виде акустической фразы, преобразуют акустическую

парольную фразу в последовательность акустических признаков, рассчитывают последовательность предопределенных речевых признаков по этой акустической фразе и определяют вариативность парольной фразы по этим признакам, после чего сравнивают определенную вариативность парольной фразы с предустановленным лимитом. 2 н. и 4 з.п. ф-лы, 7 ил.

RU 2 598 314 C 2

RU 2 598 314 C 2



Фиг.1



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(51) Int. Cl.
G10L 17/14 (2013.01)
G10L 17/24 (2013.01)
G10L 15/00 (2013.01)

(12) **ABSTRACT OF INVENTION**

(21)(22) Application: **2013136376/08, 05.08.2013**
(24) Effective date for property rights:
05.08.2013
Priority:
(22) Date of filing: **05.08.2013**
(43) Application published: **10.02.2015** Bull. № 4
(45) Date of publication: **20.09.2016** Bull. № 26
Mail address:
197227, Sankt-Peterburg, a/ja 405, Voropaju Sergeju Aleksandrovichu

(72) Inventor(s):
**KHitrov Mikhail Vasilevich (RU),
Dyrmovskij Dmitrij Viktorovich (RU)**
(73) Proprietor(s):
**Obshshestvo s ogranichennoj otvetstvennostyu
"TSentr rechevykh tekhnologij" (OOO "TSRT")
(RU)**

(54) **METHOD FOR ASSESSING VARIABILITY OF A PASS PHRASE (VERSIONS)**

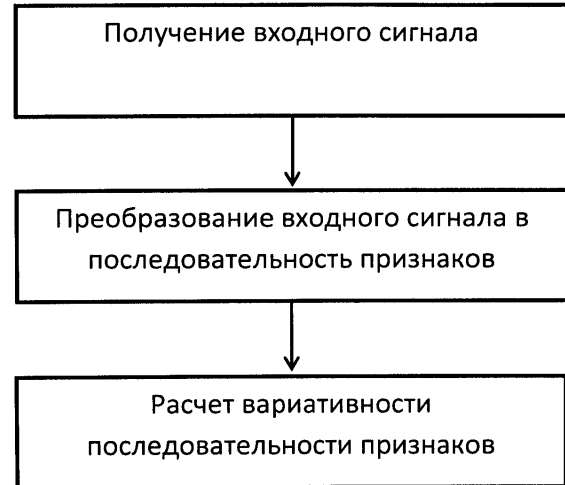
(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention relates to speech recognition. Method for assessing variability of a pass phrase comprising obtaining a pass phrase from the user and estimating its variability, characterized by the fact that a pass phrase is obtained from the user in the form of acoustic phrase, acoustic pass phrase is converted in sequence of acoustic criteria, sequence of predefined speech features is calculated by said acoustic phrase and the pass phrase variability is determined by these criteria, then certain pass phrase variability is compared with predefined limit.

EFFECT: provision of reliable evaluation of the pass phrases variability.

6 cl, 7 dwg



Фиг.1

RU 2 598 314 C2

RU 2 598 314 C2

Изобретение относится главным образом к технологиям распознавания речи, в частности к системам, сравнивающим голос пользователя с записанным голосом другого пользователя и выдающим оценку схожести голосов, и может быть использовано в системах ограничения несанкционированного доступа в помещения или информационным ресурсам.

Распознавание речи - это процесс автоматического распознавания говорящего на основании индивидуальной информации, содержащейся в звуковых сигналах. Этот процесс может быть разделен на идентификацию и верификацию. Идентификация определяет, кто именно говорит из имеющегося числа дикторов. Верификация определяет соответствие или несоответствие личности говорящего. Верификация может быть использована для контроля доступа к ограниченным сервисам, к примеру телефонный доступ к банковским операциям, совершение покупок или доступ к секретному оборудованию.

Способ использования технологии обычно представляет собой процесс, когда пользователь произносит короткую фразу в микрофон. Затем измеряются и определяются различные акустические параметры (звуки, частота, высота тона и другие физические характеристики голосовых каналов, которые обычно называют звуковыми характеристиками). Затем эти элементы используются для установления набора уникальных звуковых параметров пользователя (которые обычно называются «отпечаток голоса» или «голосовая модель»). Данный процесс обычно называют регистрацией. Регистрация в этом случае представляет собой получение образца голоса. Затем полученный образец голоса обрабатывается (трансформируется в соответствующий отпечаток голоса), и отпечаток голоса хранится совместно с идентификаторами личности для использования в протоколах безопасности. Во время процесса верификации диктору предлагается повторить фразу, которая использовалась при регистрации. Алгоритм верификации голоса сравнивает голос диктора с записью голоса, сделанной во время регистрации. Технология верификации затем принимает или отклоняет попытку диктора установить соответствие голосовому образцу. Если голосовой образец соответствует, то пользователю предоставляется защищенный доступ. Если нет - то пользователю будет отказано в предоставлении доступа. Системы верификации диктора могут быть текстозависимыми или текстонезависимыми, либо являться их комбинацией. В текстозависимых системах человек произносит заранее заданное слово или фразу. Данная информация (обычно называемая «голосовой пароль» «кодовая фраза», «голосовой отпечаток») может представлять собой такую информацию, как имя, место рождения, любимый цвет или последовательность чисел. В текстозависимых системах распознавание диктора происходит без требования заранее установленной кодовой фразы.

Для оценки новизны и технического уровня заявленного решения рассмотрим ряд известных заявителю технических средств аналогичного назначения, характеризующих совокупностью сходных с заявленным изобретением признаков, известных из сведений, ставших общедоступными до даты приоритета изобретения.

Известен способ аутентификации диктора по входному речевому сигналу диктора в виде парольной фразы, включающий сравнение параметров этого сигнала с заданной точностью с заранее сохраненными эталонами параметров входных речевых сигналов в виде той же парольной фразы, произносимой заранее известными дикторами, с последующей аутентификацией, отличающийся тем, что в качестве упомянутых параметров берется низкочастотная часть вейвлет преобразования от нормированной функции распределения особых точек вдоль звукового файла, отвечающего входному

речевому сигналу диктора в виде парольной фразы, выделенных сравнением отсчета в этой точке в звуковом файле с предшествующими и последующими отсчетами посредством обобщенных коэффициентов линейного предсказания и порога T , при этом нормирование функции распределения сводится к приведению ее к стандартной длине L_{ep} , принятой при подсчете эталонных параметров входных речевых сигналов в виде парольной фразы, произносимой заранее известным дикторами, см. патент РФ №2422921.

Известен способ аутентификации диктора по парольной фразе, включающий посегментное сравнение входного речевого сигнала диктора с заранее сохраненными эталонами параметров эталонных фраз, произносимых заранее известными дикторами, для чего осуществляют сравнение параметрических описаний последовательных сегментов входного речевого сигнала с параметрическими описаниями последовательных сегментов из выбранных для сравнения с упомянутым эталоном с последующей аутентификацией диктора, отличающийся тем, что в качестве упомянутых параметрических описаний берут матрицу переходов, построенную в соответствии с правилом, заключающимся в том, что строят последовательность особых точек, выделенных сравнением отсчета в сегменте с окружением отсчета, определенным посредством обобщенных коэффициентов линейного предсказания и порога T , далее агрегируют последовательности особых точек в блоки длины L , строят матрицу переходов, аналогичную матрице переходов в цепи Маркова, по числу особых точек в блоке и сравнивают полученную матрицу с образцом эталонной матрицы с заданной точностью и принимают решение о правильности аутентификации диктора, см. патент РФ №2422920.

Существуют определенное число различных технологий, используемых для создания голосовых отпечатков: скрытые модели Маркова (HMMs), Gaussian Mixture Models (GMMs), искусственные нейронные сети или совокупности вышеуказанных техник. Одной из проблем с вышеописанной технологией распознавания является вариативность голосового пароля (кодовой фразы, голосового отпечатка). Кодовая фраза может быть фонетически богата или фонетически скудна. «Фонетически скудная кодовая фраза» означает, что эта кодовая фраза содержит только ограниченное количество уникальных звуков (фонем) и, соответственно, вариативность этой кодовой фразы мала. Если вариативность кодовой фразы мала (в крайних случаях кодовая фраза содержит только набор идентичных звуков, например, «а-а-а-а»), невозможно оценить соответствующие физические характеристики голосовых каналов диктора. В результате создается неэффективный голосовой отпечаток и эффективность системы распознавания диктора резко снижается.

Необходимо отметить, что эта проблема отличается от проблемы криптографической защищенности текстового пароля. В самом деле, если голосовой пароль содержит ограниченное число уникальных текстовых знаков (в крайних случаях кодовая фраза содержит только набор идентичных знаков, например, «qqqq»), его криптографическая защищенность существенно низка. Однако это означает только, что пароль может быть легко угадан и является недостаточно сложным, чтобы отразить криптографические атаки.

В противоположность этому система распознавания диктора не может создать эффективные голосовые отпечатки в связи с недостатком звуков в кодовой фразе. Результатом слабого голосового отпечатка в процессе верификации или идентификации является низкое качество распознавания диктора. К примеру, одним из обычно используемых коэффициентов вероятности для оценки работы системы распознавания

является Уровень равновероятной ошибки (Equal Error Rate - EER). Чем ниже EER, тем лучше система распознавания. Было установлено, что EER увеличивается с 6% для фонетически богатых парольных фраз до 18% для фонетически скудных парольных фраз.

5 Задача изобретения заключается в создании способа для оценки вариативности парольной фразы, которая могла бы быть затем использована для генерирования фонетически богатых паролей в текстозависимых системах распознавания, для оценки вариативности входных данных парольной фразы в текстозависимой системе при регистрации и для генерирования предупреждения диктора в случае низкой
10 вариативности парольной фразы. Определение вариативности парольной фразы затем может быть использовано для генерации фонетически представительных паролей в текстозависимых системах идентификации диктора по голосу, для оценки вариативности входной фразы в текстонезависимых системах в процессе регистрации и для генерации предупредительного сообщения клиенту в случае низкой вариативности парольной
15 фразы.

Сущность первого независимого объекта заявляемого изобретения как технического решения выражается в следующей совокупности существенных признаков, достаточной для достижения указанного выше обеспечиваемого изобретением технического результата.

20 Согласно первому независимому объекту изобретения способ оценки вариативности парольной фразы, включающий получение парольной фразы от пользователя и оценку ее вариативности, характеризующийся тем, что получают от пользователя парольную фразу в виде акустической фразы, преобразуют акустическую парольную фразу в последовательность акустических признаков, рассчитывают последовательность
25 предопределенных речевых признаков по этой акустической фразе и определяют вариативность парольной фразы по этим признакам, после чего сравнивают определенную вариативность парольной фразы с предустановленным лимитом.

В этом заключается совокупность существенных признаков первого независимого варианта изобретения, обеспечивающая получение технического результата во всех
30 случаях, на которые распространяется испрашиваемый объем правовой охраны.

Кроме того, первой независимый вариант изобретения характеризуется наличием ряда факультативных признаков, описывающих частные случаи его реализации, а именно:

- преобразование акустической парольной фразы в последовательность акустических
35 признаков осуществляют путем преобразования парольной фразы в последовательность спектров, после чего преобразуют спектры в первую последовательность формантов;
- вариативность парольной фразы определяют по оценке гистограмм N-Dim для каждой траектории формант, затем оценивают минимальные и максимальные значения для каждой форманты, выводят по меньшей мере одну совокупности бинов гиперкуба,
40 определяют место каждой форманты как единицы в соответствующей совокупности бинов гиперкуба и используют гистограммы N-Dim для оценки энтропии и максимального значения данной энтропии;
- оценивают абсолютную псевдоэнтропию;
- оценивают относительную псевдоэнтропию.

45 Согласно второму независимому объекту изобретения способ оценки вариативности парольной фразы, включающий получение парольной фразы от пользователя и оценку ее вариативности, характеризующийся тем, что получают от пользователя текстовую парольную фразу, преобразуют текстовую парольную фразу в последовательность

фонетических символов и определяют вариативность текста парольной фразы по последовательности фонетических символов, после чего сравнивают определенную вариативность парольной фразы с предустановленным лимитом.

5 За счет реализации отличительных признаков изобретения достигается технический результат, заключающийся в том, что, заявленный способ в обоих вариантах его реализации обеспечивает надежную оценку вариативности парольных фраз, полученных как в акустическом, так и в текстовом виде.

10 Сущность изобретения поясняется чертежами, где на фиг. 1 представлена блок-схема реализации заявленного способа в обоих вариантах, на фиг. 2 - схема реализации первого варианта заявленного способа, при получении парольной фразы в фонетическом виде, на фиг. 3 - схема реализации второго варианта заявленного способа, при получении парольной фразы в текстовом виде, на фиг. 4 - график зависимости Equal Error Rate (EER) от информационной вариативности, на фиг. 5 - график зависимости Equal Error Rate (EER) от относительной вариативности на фиг. 6 - график зависимости Equal Error Rate (EER) от абсолютной вариативности, 1-й взвешенной (оцененной) суммы и 2-й взвешенной (оцененной) вариативности, на фиг. 7 - таблицы, иллюстрирующие числовые данные Equal Error Rate (EER) как функцию различных вариативностей.

Заявленный способ реализуют следующим образом.

20 В первом варианте получают от пользователя парольную фразу в виде акустической фразы, преобразуют акустическую парольную фразу в последовательность акустических признаков, рассчитывают последовательность предопределенных речевых признаков по этой акустической фразе и определяют вариативность парольной фразы по этим признакам, после чего сравнивают определенную вариативность парольной фразы с предустановленным лимитом.

25 Преобразуют акустическую парольную фразу в последовательность акустических признаков, осуществляют путем преобразования парольной фразы в последовательность спектров, после чего преобразуют спектры в первую последовательность формантов. Вариативность парольной фразы определяют по оценке гистограмм N-Dim для каждой траектории формант, затем оценивают минимальные и максимальные значения для каждой форманты, выводят по меньшей мере одну совокупности бинов гиперкуба, определяют место каждой форманты как единицы в соответствующей совокупности бинов гиперкуба и используют гистограммы N-Dim для оценки энтропии и максимального значения данной энтропии. Оценивают абсолютную и относительную псевдоэнтропию.

35 Во втором варианте получают от пользователя текстовую парольную фразу, преобразуют текстовую парольную фразу в последовательность фонетических символов и определяют вариативность текста парольной фразы по последовательности фонетических символов, после чего сравнивают определенную вариативность парольной фразы с предустановленным лимитом.

40 Устройство, реализующее оба варианта заявленного способа, представляет собой взаимосвязанные носитель информации, центральный процессор и графический интерфейс, где на носителе информации имеются машинные команды, включающие команды на получение парольной фразы от пользователя, расчета последовательности предопределенных акустических признаков или фонетических символов, оценки вариативности парольной фразы на основе этих признаков, сравнение рассчитанной вариативности парольной фразы с предопределенным порогом и сообщение пользователю результата сравнения значения вариативности парольной фразы с предопределенным порогом.

Данное устройство может быть реализовано с использованием известных компьютерных или мультипроцессорных систем.

Формула изобретения

5 1. Способ оценки вариативности парольной фразы, включающий получение парольной фразы от пользователя и оценку ее вариативности, отличающийся тем, что получают от пользователя парольную фразу в виде акустической фразы, преобразуют акустическую парольную фразу в последовательность акустических признаков, рассчитывают последовательность предопределенных речевых признаков по этой
10 акустической фразе и определяют вариативность парольной фразы по этим признакам, после чего сравнивают определенную вариативность парольной фразы с предустановленным лимитом.

2. Способ по п. 1, отличающийся тем, что преобразование акустической парольной фразы в последовательность акустических признаков осуществляют путем
15 преобразования парольной фразы в последовательность спектров, после чего преобразуют спектры в первую последовательность формантов.

3. Способ по п. 1, отличающийся тем, что вариативность парольной фразы определяют по оценке гистограмм N-Dim для каждой траектории формант, затем оценивают минимальные и максимальные значения для каждой форманты, выводят
20 по меньшей мере одну совокупности бинов гиперкуба, определяют место каждой форманты как единицы в соответствующей совокупности бинов гиперкуба и используют гистограммы N-Dim для оценки энтропии и максимального значения данной энтропии.

4. Способ по п. 1, отличающийся тем, что оценивают абсолютную псевдоэнтропию.

5. Способ по п. 1, отличающийся тем, что оценивают относительную псевдоэнтропию.

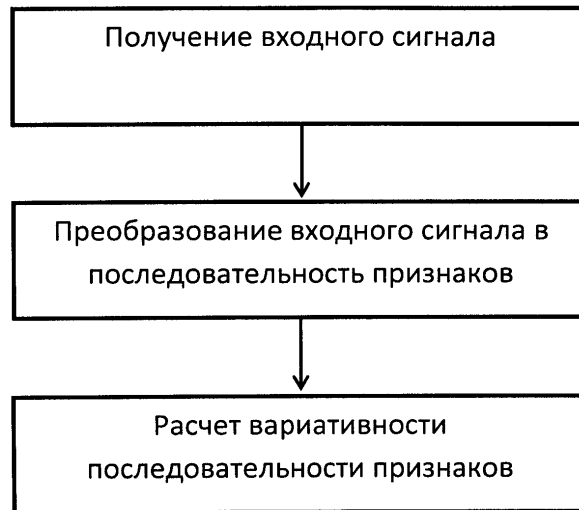
25 6. Способ оценки вариативности парольной фразы, включающий получение парольной фразы от пользователя и оценку ее вариативности, отличающийся тем, что получают от пользователя текстовую парольную фразу, преобразуют текстовую парольную фразу в последовательность фонетических символов и определяют вариативность текста парольной фразы по последовательности фонетических символов,
30 после чего сравнивают определенную вариативность парольной фразы с предустановленным лимитом.

35

40

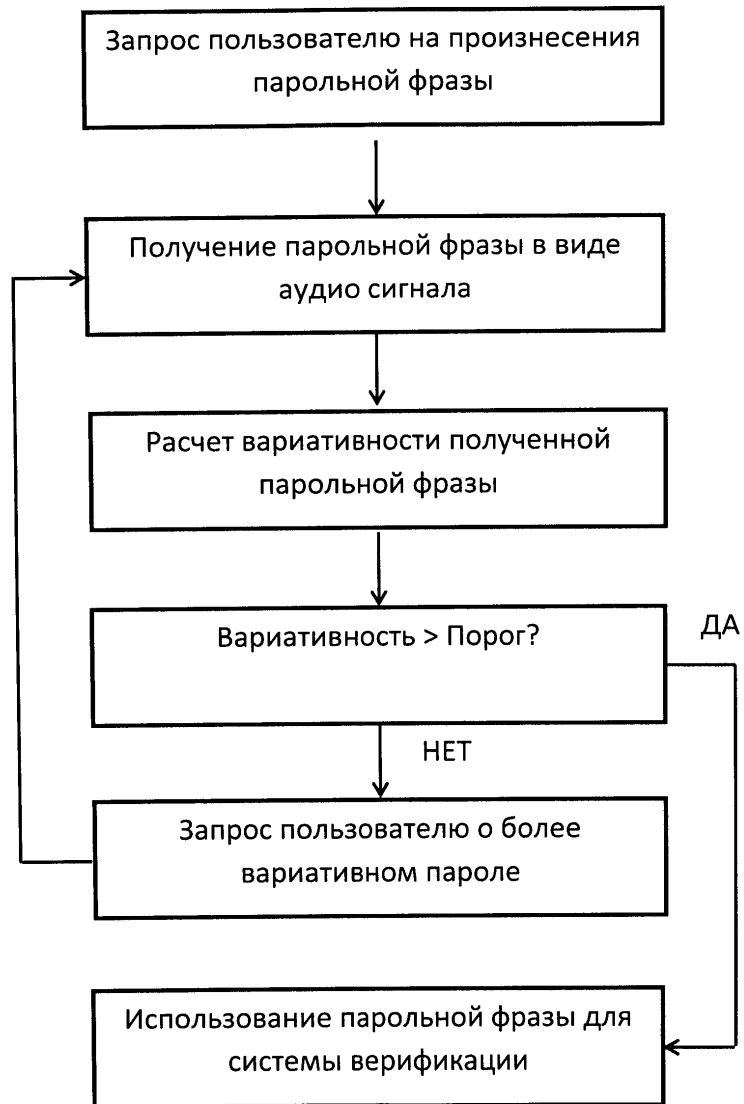
45

**Способ оценки вариативности парольной фразы
(варианты)**



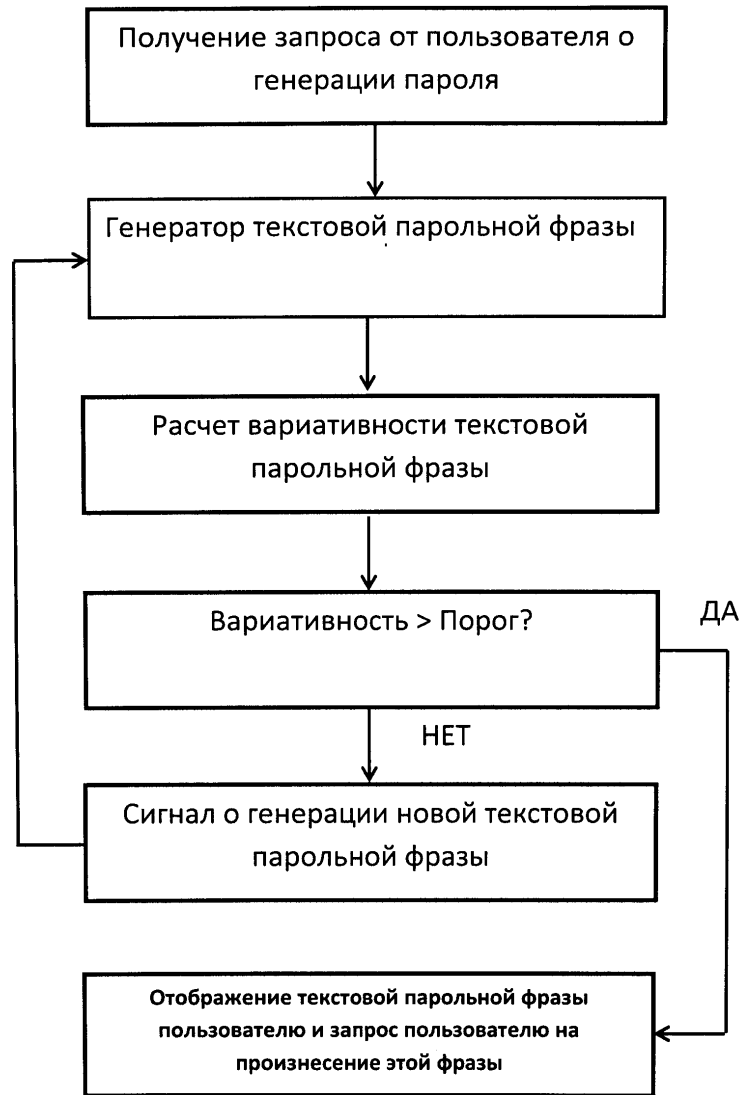
Фиг.1

**Способ оценки вариативности парольной фразы
(варианты)**



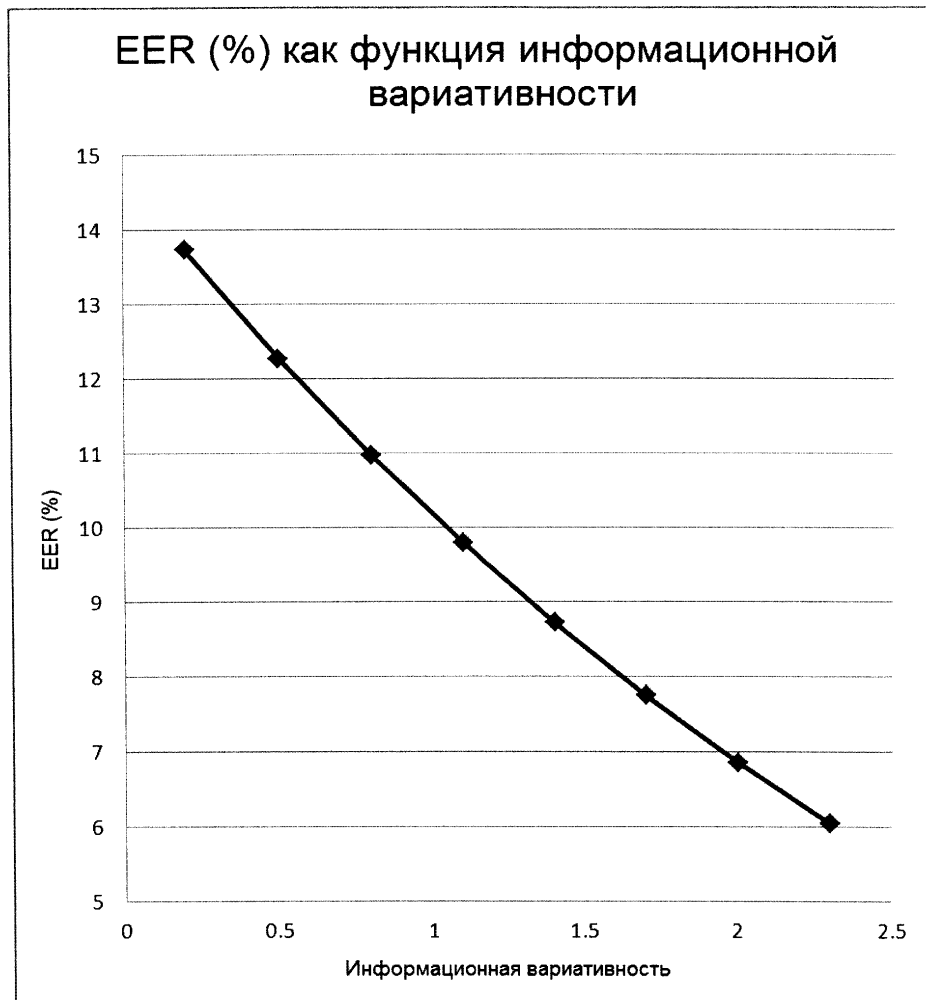
Фиг.2

**Способ оценки вариативности парольной фразы
(варианты)**



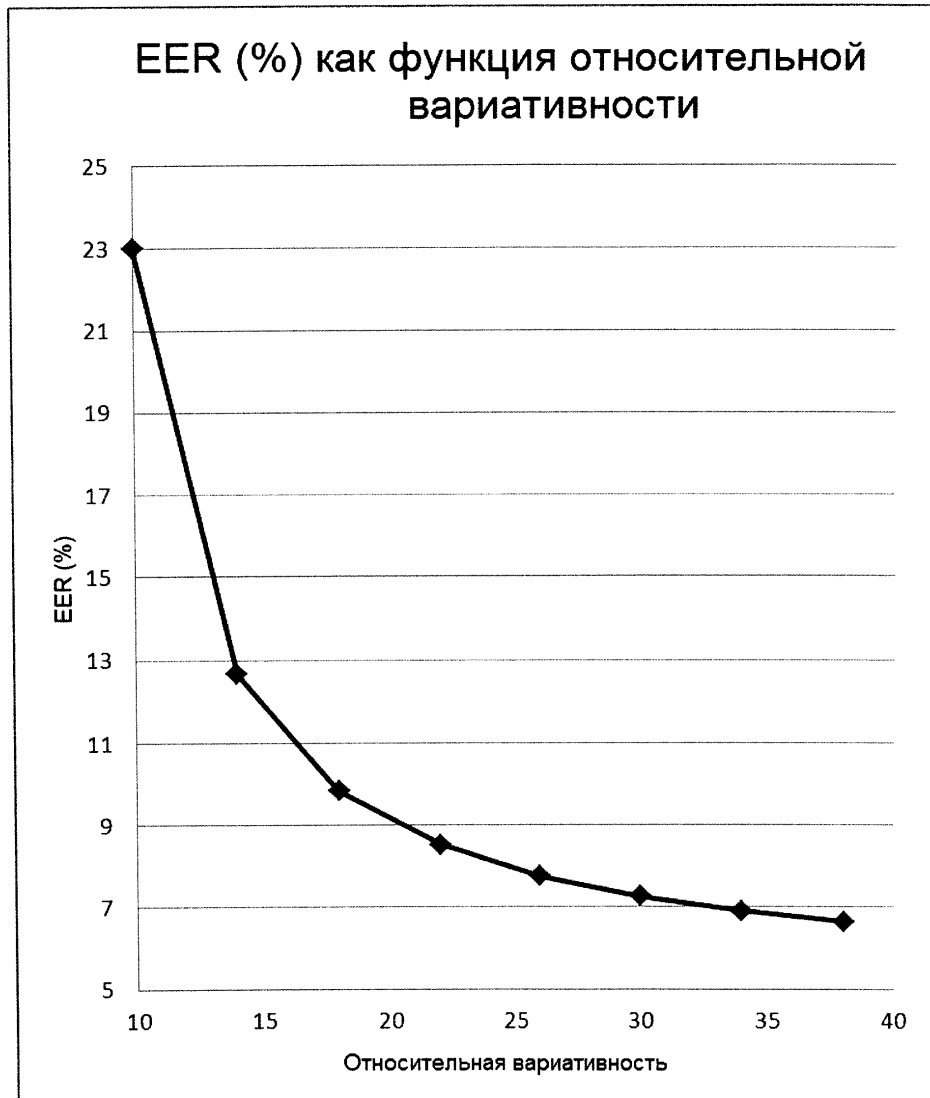
Фиг.3

Способ оценки вариативности парольной фразы
(варианты)



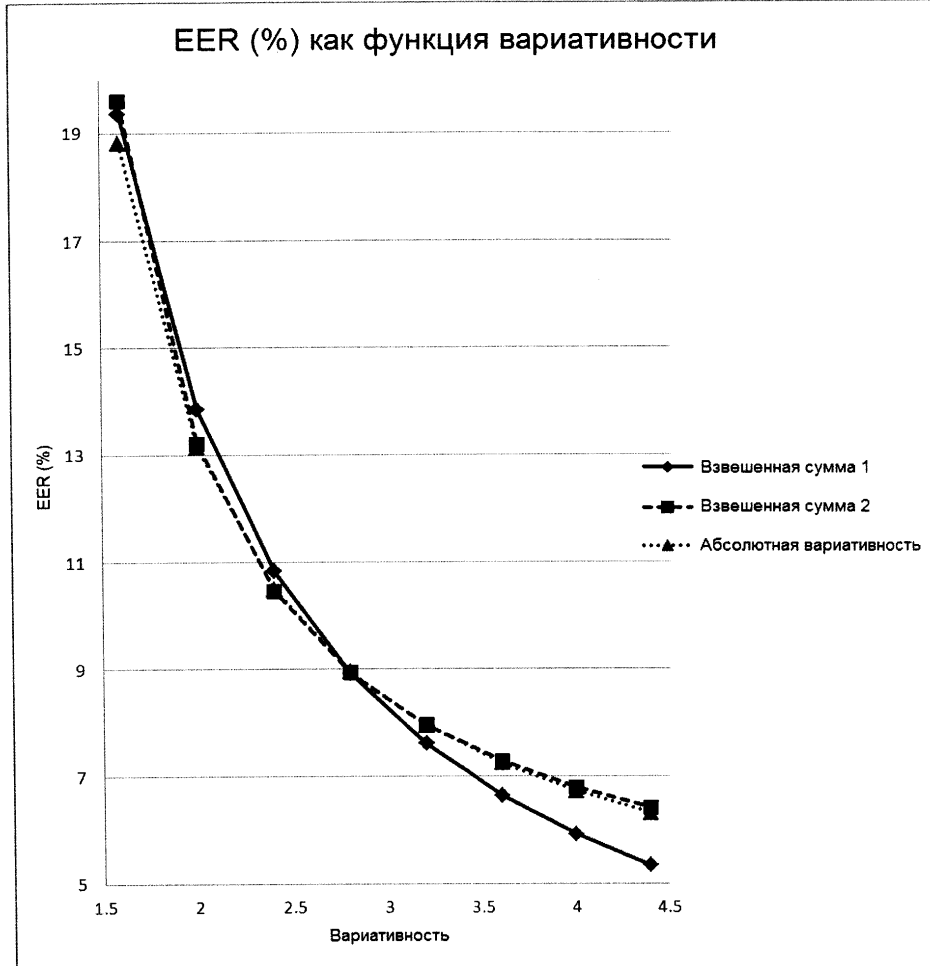
Фиг.4

Способ оценки вариативности парольной фразы
(варианты)



Фиг.5

Способ оценки вариативности парольной фразы
(варианты)



Фиг. 6

**Способ оценки вариативности парольной фразы
(варианты)**

Таблица 1

Информационная вариативность	EER %
0.2	13.73
0.5	12.27
0.8	10.97
1.1	9.79
1.4	8.72
1.7	7.75
2	6.86
2.3	6.04

Таблица 2

Относительная вариативность	EER %
10	23
14	12.66
18	9.84
22	8.52
26	7.76
30	7.26
34	6.91
38	6.65

Таблица 3

Вариативность	EER % взвешенной суммы 2	EER % для взвешенной суммы 1	EER % абсолютная вариативность
1.6	19.36	19.6	18.81
2	13.85	13.2	13.14
2.4	10.83	10.46	10.49
2.8	8.92	8.93	8.95
3.2	7.61	7.96	7.95
3.6	6.65	7.29	7.25
4	5.92	6.8	6.73
4.4	5.34	6.42	6.32

Фиг.7