УДК 004.9

Е.А. Андреева

Система аутентификации, основанная на использовании акустических свойств сердца

Идентификация и аутентификация пользователя в системе являются одними из важных задач информационной безопасности. С помощью данных процедур осуществляется управление доступом в информационное пространство. Но с развитием информационных технологий становится важно не только проверять подлинность пользователя на входе в систему, но и контролировать его аутентичность во время работы в системе, для того чтобы исключить возможность осуществления несанкционированного доступа от лица авторизованного пользователя. Для решения этой задачи необходимо непрерывно проводить аутентификацию пользователя в системе. В статье предложена модель системы аутентификации, которая обеспечивает постоянный контроль авторизованного пользователя. В качестве самой процедуры аутентификации предложено использовать биометрическую технологию, основанную на акустических свойствах сердца. Такой метод отличается от других способов аутентификации и применительно к системе, рассмотренной в данной статье, имеет ряд преимуществ.

Ключевые слова: непрерывная система аутентификации, биометрия, акустические свойства сердца.

Модель системы аутентификации

Модель функционирования системы аутентификации представлена на рис. 1. Система обладает следующими свойствами:

- непрерывное накопление биометрических данных;
- непрерывная аутентификация;
- непрерывное обновление биометрических данных;
- непрерывное ведение статистики.

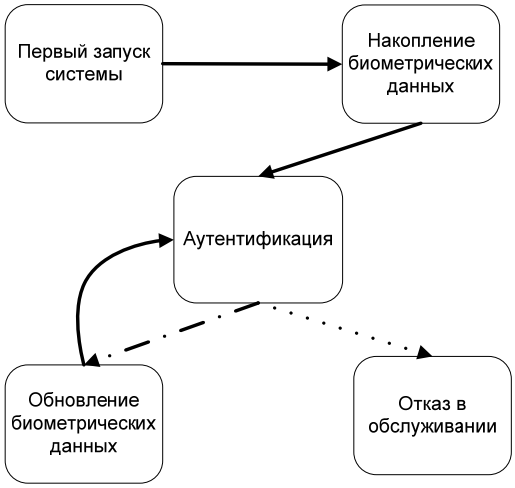

Рис. 1. Модель функционирования системы аутентификации

В данной системе процедура аутентификации должна происходить независимо от действий пользователя, но при этом оставаться надежной и устойчивой к атакам. Эти факторы играют решающую роль при выборе метода аутентификации для данной системы. Но прежде чем перейти к рассмотрению выбранного метода, приведем сравнительную характеристику современных способов аутентификации.

Современные способы аутентификации

Способы аутентификации можно разделить на три категории:

- пароль – аутентификация с помощью информации, которую знает пользователь;
- устройство аутентификации – аутентификации с помощью устройства, которым обладает пользователь;
- биометрия – аутентификация с помощью особой физической или психологической черты, которой обладает пользователь.

Биометрия является наиболее простым способом аутентификации с точки зрения пользователя. Нет необходимости запоминать пароль или носить с собой устройство аутентификации. Но, с другой стороны, биометрия – наиболее дорогостоящий и сложный в реализации метод аутентификации. Выбор метода аутентификации зависит от свойств и характеристик конкретной системы.

В табл. 1 представлена сравнительная характеристика методов аутентификации, которые можно применить в рассмотренной системе аутентификации.

Таблица 1

Сравнительная характеристика современных способов аутентификации

Название	Преимущества	Недостатки
Пароль	Простота использования	Возможность потери и кражи. Обязательная процедура ввода данных
Устройство аутентификации (ключ)	Простота использования	Возможность потери и кражи. Обязательная процедура ввода данных
Отпечаток пальца	Высокая точность аутентификации. Надежность	Биометрическая характеристика может быть утрачена или повреждена. Обязательная процедура ввода данных
ДНК	Высокая точность аутентификации. Надежность. Необязательная процедура ввода данных	Сложная процедура анализа. Сложная процедура ввода данных
Голос	Простота использования. Простота сбора данных	Возможность подмены. Обязательная процедура ввода данных

Из таблицы видно, что в большинстве способов аутентификации требуется обязательная процедура ввода данных, поэтому их невозможно применять в данной системе. Без процедуры ввода данных можно обойтись в случае аутентификации по ДНК, но ДНК-анализ является сложным и долгим, поэтому эта технология также исключается из рассмотрения.

Метод аутентификации с использованием акустических свойств сердца

В качестве метода аутентификации в рассмотренной системе предлагается использовать биометрическую технологию, основанную на акустических свойствах сердца. В тонах сердца содержится уникальная информация, поэтому они могут быть использованы как биометрическая характеристика человека.

Данная технология отличается от остальных следующими свойствами:

- тоны сердца не могут быть утрачены в течение жизни;
- тоны сердца сложно подделать;
- аутентификация может производиться без действий пользователя.

Но сложность данной технологии состоит в том, что звуки сердца могут изменяться в течение жизни.

На рис. 2 представлены сигналы сердцебиения для пяти разных людей. Они обладают периодичностью и отличаются друг от друга.

Спектры сигнала сердцебиения одного человека, отличаются характерной формой, которая сохраняется при изменении интенсивности или темпе сигнала. Это важно, потому что частотные характеристики человека могут быстро меняться во времени в зависимости от его физического или эмоционального состояния. Но неизменной остается «мелодия» сердцебиения, т.е. последовательность смены частот в спектре.

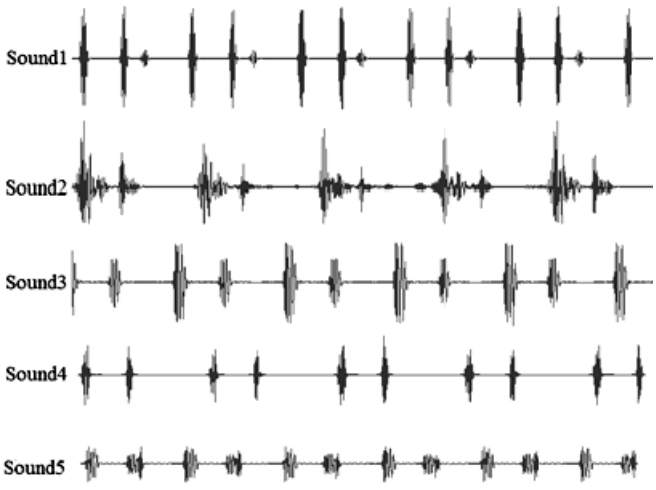

Рис. 2. Звуки сердцебиения пяти разных людей

При аутентификации важно решить две задачи:

- отличить сигналы сердцебиения для двух разных людей;
- распознать сигнал сердцебиения для одного человека, но с изменившимися характеристиками.

Алгоритм сравнения двух сигналов сердцебиения:

1. Разбиение спектра сигнала на области (1, …, n) .
2. Нахождение максимума спектра.
3. Разбиение спектра на уровни (1, …, q) .
4. Нахождение максимума для каждой области спектра.
5. Составление кодового слова, в котором длина равна n, а значение равно номеру уровня, в который попадает максимум спектра.
6. Анализ кодовых слов с целью определения формы спектра.

На рис. 3 представлена схема разбиения спектра на области и на уровни.

Номер уровня определяет значение в ячейке кодового слова. В табл. 2 представлены кодовые слова для разных сигналов. Первые три последовательности являются частями кодового слова для сигнала сердцебиения одного человека. Сигналы для одного человека взяты с разными частотными характеристиками. Видно, что значения в ячейках не очень отличаются даже при использовании грубого метода оцифровки сигнала. Четвертая последовательность получена для сигнала другого человека. Она отличается от первых трех, что позволяет отличить данный сигнал от остальных.

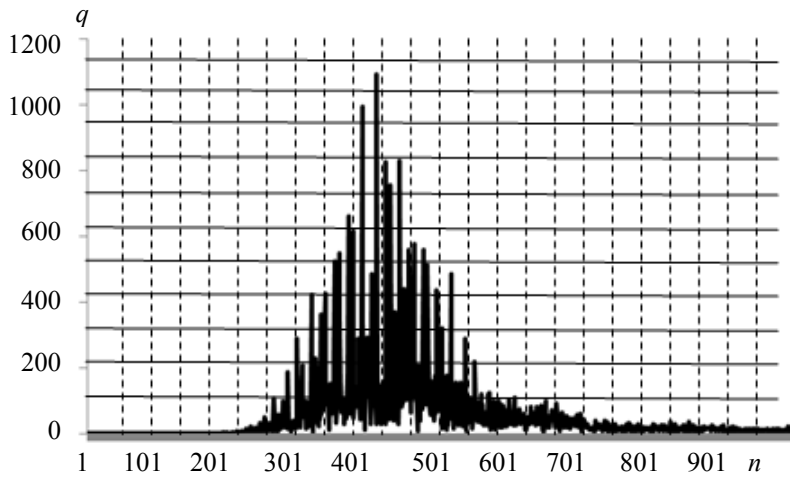

Рис. 3. Спектр сигнала сердцебиения разбитый на области и уровни

Таблица 2

Части кодовых последовательностей звуков сердцебиений

Набор звуков	Значения q для областей n на частотах от 300 до 600						
Звук сердцебиения №1 Нормальные характеристики	14	15	16	17	20	19	18
Звук сердцебиения №1 Ускорение темпа	9	12	18	20	15	10	9
Звук сердцебиения №1 Увеличение громкости	8	11	16	18	20	15	16
Звук сердцебиения №2	2	5	0	0	9	9	9

Заключение

В статье предложена система аутентификации, с помощью которой можно осуществить непрерывный контроль авторизованного пользователя в системе.

Показан метод использования акустических свойств сердца для осуществления процедуры аутентификации. С помощью данного метода можно проводить аутентификацию пользователя независимо от его действий.

Данная биометрическая технология дает также возможность контролировать состояния пользователя при работе в системе. Изучение данного вопроса является задачей для дальнейших исследований.

Литература

1. Beritelli F. Human identity verification based on heart sounds: recent advances and future directions / F. Beritelli, A. Spadaccini. – University of Catania, Italy, 2010. – P. 1–18 [Электронный ресурс]. – Режим доступа: http://cdn.intechopen.com, свободный (дата обращения: 02.04.2012).

2. Phua K. Human identification using heart sound / K. Phua, T. Dat, J. Chen L. Shue. – Singapore: Institute for Infocomm Research, 2008. – P. 1–6 [Электронный ресурс]. – Режим доступа: http://mmua.cs.ucsb.edu, свободный (дата обращения: 02.04.2012).

3. Nigam V. Cardiac Sound Separation / V. Nigam, R. Priemer. – Chicago: University of Illinois, 2004. – P. 1–4 [Электронный ресурс]. – Режим доступа: http://www.cinc.org, свободный (дата обращения: 02.04.2012).

Андреева Екатерина Александровна
Студентка каф. комплексной защиты информации
Санкт-Петербургского университета аэрокосмического приборостроения
Тел.: 8 (921) 355-51-99
Эл. почта: eandreeva89@gmail.com

Andreeva E.A.
Authentication system using heart sound as biometric

User identification and authentication in system are the most important problems of information security. These procedures realize access control to information. But with development of information technology become important not only authenticate user in the beginning of work with system, but also control his authenticity during working. The solution of this problem may be a system with continuous authentication.
Continuous authentication it is such type of authentication when system control user access at each time interval. In this paper I propose model of authentication system using heart sound to access control.
Keywords: authentication system, biometrics, access control.
