УДК 004.9

Е. А. Андреева – студентка кафедры технологии защиты информации
С. В. Беззатеев (д-р техн. наук, доц.) – научный руководитель

СИСТЕМА НЕПРЕРЫВНОЙ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ АКУСТИЧЕСКИХ СВОЙСТВ СЕРДЦА

Контроль доступа пользователя в систему является одной из важных задач информационной безопасности. Основными инструментами контроля доступа являются процедуры идентификации и аутентификация. С их помощью осуществляется проверка пользователя на входе 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 к конфиденциальной информации в течении открытого сеанса.

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.

Модель системы аутентификации

Модель функционирования системы непрерывной аутентификации представлена на рисунке 1 [1]. Система обладает следующими свойствами:

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

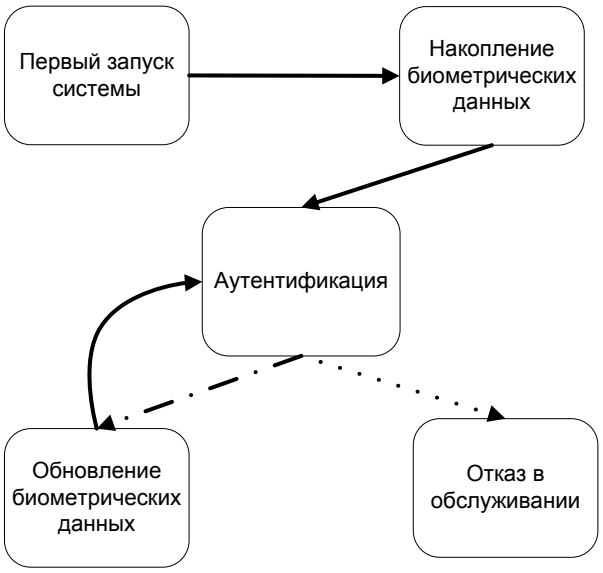

Рис. 1. Модель функционирования системы аутентификации

В данной системе процедура аутентификации должна происходить независимо от действий пользователя (то есть быть не активной), 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 [2]:

- 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 таблице 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 активная процедура ввода данных;
Отпечаток пальца	Высокая точность аутентификации; Надежность;	Биометрическая характеристика может быть утрачена или повреждена; Обязательная активная 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 активная процедура ввода данных;

Из таблицы видно, что в большинстве способов аутентификации требуется обязательная активная процедура ввода данных, поэтому их невозможно применять в данной системе. Без активной 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 [3].

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.

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 эмоцио-

нального состояния. Но неизменной остается «мелодия» сердцебиения, то есть последовательность смены частот в спектре.

При аутентификации важно решить две задачи [4]:

– отличить сигналы сердцебиения для двух разных людей;

– распознать сигнал сердцебиения для одного человека, но с изменившимися характеристиками.

Выделение информационных коэффициентов звукового сигнала сердца

Для того чтобы провести более глубокие исследования в данном вопросе, был разработан метод выделения индивидуальных характеристик звуковых сигналов сердца. В данном подходе использованы стандартные шаги алгоритмов распознавания речи, но с учетом особенностей звука сердцебиения.

На схеме показаны основные блоки метода распознавания звуков сердцебиения.

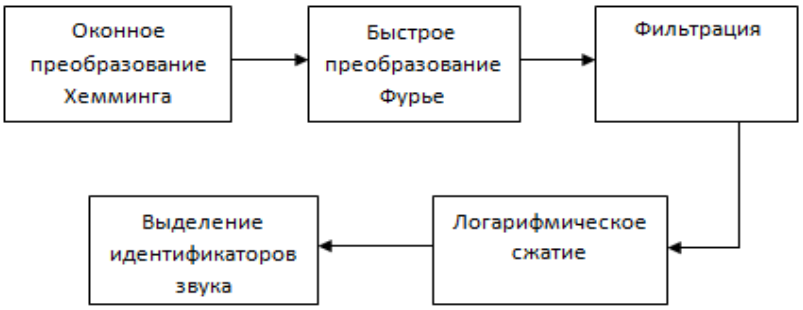

Рис. 2. Алгоритм выделения идентификаторов звукового сигнала

Идентификаторами звука здесь названы информационные коэффициенты сигнала, полученные после прохождения всех шагов алгоритма. С помощью сравнения информационных коэффициентов в каждой области частот спектра можно определить, насколько один звуковой сигнал сердца отличается от другого.

Схема классификации информационных коэффициентов звукового сигнала сердца

Для того чтобы определить соответствует ли звуковой сигнал сердца конкретному человеку, нужно сформировать критерии для принятия решений. Этими критериями будут служить верхняя и нижняя границы допустимости.

Пользователь не проходит аутентификацию
Верхняя граница
Область неопределенности
Нижняя граница
Пользователь проходит аутентификацию

Рис. 3: Схема классификации информационных коэффициентов звуковых сигналов сердца

Верхняя граница допустимости определяет значение, с которым сравнивается разница между эталонным и новым сигналом, поступившим в биометрическую систему при аутентификации. Если разница между сигналами больше чем верхняя граница, то пользователю отказывается в доступе в систему, так как сигнал распознается, как сердцебиение постороннего человека.

Нижняя граница допустимости определяет максимальное значение разницы в сигналах сердцебиения одного человека. Если полученное значение меньше нижней границы, то человек проходит процедуру аутентификации, и дальше может производиться анализ состояния человека, с целью определения его физического и психологического состояния.

Значение верхней границы определяется в ходе исследований и может быть использовано для

большого набора сигналов, в то время как значение нижней граница можно определить только после сбора статистики для конкретного человека, так как пределы изменения звуковых характеристик сердца для разных людей значительно отличаются.

Формирование кодовых последовательностей

Для упрощения процедуры аутентификации каждому сигналу присваивается кодовое слово $\vec{v}$. Длина кодового слова ровняется количеству областей, на которые разбивается спектр сигнала при подсчете информационных коэффициентов, а значения принадлежат множеству [0;1].

Процедура аутентификации выполняется в два этапа. На первом этапе по формуле (1) вычисляется кодовое слово $\vec{v}^A$.

$$v_i^A = \begin{cases} 1, & \text{если } w_i > MAX \\ 0, & \text{если } w_i < MAX \end{cases}, \quad (1)$$

где $w_i -$ значение разницы между информационными коэффициентами двух сигналов для определенной области частот, а MAX - значение верхней границы допустимости. После вычисления значений кодового слова для всех областей частот, для него определяется вес Хемминга (W). Если вес Хемминга больше или равен значения, установленного в системе, то пользователь не проходит процедуру аутентификации. Если меньше, то система переходит ко второму этапу аутентификации, на котором вычисляется кодовое слово $\vec{v}^B$ по формуле (2).

$$v_i^B = \begin{cases} 1, & \text{если } w_i > MIN \\ 0, & \text{если } w_i < MIN \end{cases}, \quad (2)$$

где MIN – значение нижней границы. После вычисления значений кодового слова $\vec{v}^B$ повторно определяется вес Хемминга и сравнивается со значением, установленным в системе. Вес Хемминга для кодовых слов $\vec{v}^A$ и $\vec{v}^B$ может не совпадать и определяется в ходе исследований. Если вес Хемминга $\vec{v}^B$ меньше значения установленного в системе, то пользователь проходит процедуру аутентификации и допускается к работе в системе. В противном случае пользователю будет отказано в аутентификации, так как сигнал попадет в область неопределенности и будет рассмотрен отдельно.

В ходе исследований были рассчитаны значения показателей эффективности биометрической системы при различных значениях веса Хемминга для кодовых слов $\vec{v}^A$ и $\vec{v}^B$. В качестве показателей эффективности системы выбраны:

- FAR – коэффициент ложного приема данных;
- FRR – коэффициент ложного отказа доступа системы.

Значение верхней границы допустимости выбрано, как $MAX = 4000$, а нижней границы, как $MIN = 400$. Эти значения определены в ходе проведенных исследований. Относительная рабочая характеристика системы при заданных значениях показана на графиках.

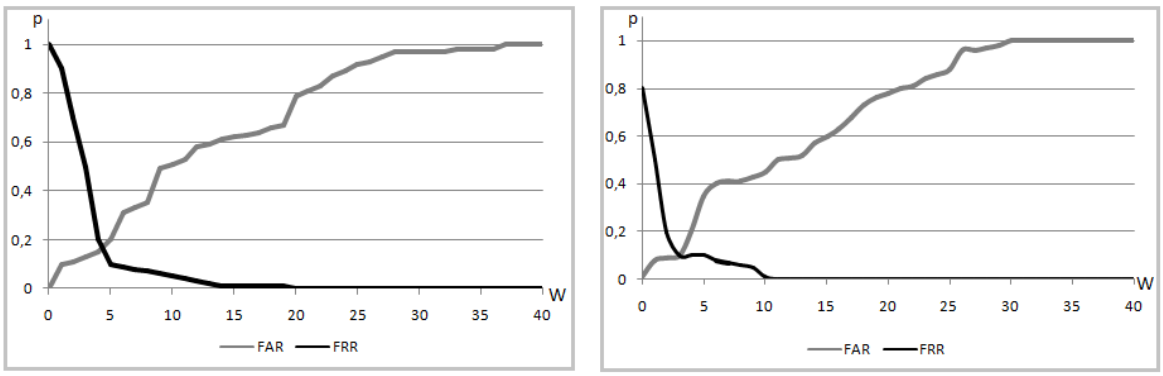

Рис. 4: Расчет относительной рабочей характеристики системы для кодового слова $\vec{v}^A$ (слева), расчет относительной рабочей характеристики системы для кодового слова $\vec{v}^B$ (справа)

Точка пересечения графиков – это компромисс между характеристиками FAR и FRR, который по-

казывает оптимальные значения веса Хемминга для кодовых слов $\vec{v}^A$ и $\vec{v}^B$. Наилучшие результаты биометрической системы были получены при значениях $W_{(A)} = 5$ для $\vec{v}^A$ и $W_{(B)} = 3$ для $\vec{v}^B$.

Заключение

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

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

Описанная биометрическая технология дает возможность контролировать состояния пользователя при работе в системе.

Библиографический список

1. Андреева Е.А. Непрерывная аутентификация, использующая фонокардиографический метод. − XXIV всероссийская научно-техническая конференция студентов, молодых ученых и специалистов «Биотехнические, медицинские и экологические системы и комплексы», Рязанский Государственный Радиотехнический Университет, 2012.
2. Beritelli F, Spadaccini A. Human Identity Verification Based on Heart Sounds: Recent Advances and Future Directions. − University of Catania, Italy 2010
3. Phua K, Dat T H, Chen J, Shue L. Human identification using heart sound. − Institute for Infocomm Research, Singapore 2008
4. Biometrics: Publications http://biometrics.cse.msu.edu