УДК 519.254

М.В. ОВСЕЕНКО, магистр НТУ «ХПИ»,
В.Н. БАЛЕВ, канд. техн. наук, доц. НТУ «ХПИ»

ПОСТРОЕНИЕ СИСТЕМЫ АВТОРИЗАЦИИ ПО ГОЛОСУ И ИЗУЧЕНИЕ АЛГОРИТМОВ ЕЁ РАБОТЫ

У статті розглянуті методи аутентифікації, зокрема біометричні, серед яких найбільша увага надається авторизації за голосом. Також у статті наведено опис дослідницької роботи та структури приладу.

В статье рассмотрены методы аутентификации, в частности биоматематические, среди которых наибольшее внимание предоставляется авторизации за голосом. Также в статье приведено описание исследовательской работы и структуры прибора.

The article deals with methods of authentication, including biometrics, among which the most attention is given authorization vote. This article also describes the research and structure of the device.

Перед любым предприятием в современном мире остро стоит проблема защиты от несанкционированного доступа к своим материальным (помещения, здания) и виртуальным (файлы, базы данных) ресурсам. Для ее решения применяются различные системы разграничения доступа. Важным элементом такой системы разграничения доступа является способ авторизации (подтверждения подлинности личности) пользователя. Самым простым в реализации способом подтверждения прав доступа к материальному ресурсу или объекту является использование механического замка с ключом, а к виртуальному — пароля доступа. Однако существуют и другие, более современные и надежные, методы подтверждения прав доступа.

Виды авторизации

1. Однофакторная авторизация

При однофакторной авторизации для получения прав доступа к какому-либо ресурсу достаточно предоставить системе одно (любое утвержденное) подтверждение своих прав. Все используемые в этом случае методы авторизации можно разделить на три вида:

1.1 Знания человека. Доступ к ресурсу предоставляется на основании информации, известной человеку. Например, для доступа к компьютерной системе может использоваться имя пользователя (login) и парольная фраза. Вариантом этого метода служит система с однократными паролями (one time passwords), когда человек знает не сам пароль, а алгоритм его получения по данным, предоставленным системой.

1.2 Объекты владения. У пользователя, желающего получить доступ к системе, есть некий материальный объект: брелок с записанным в него электронным ключом, бумажный пропуск со штрих-кодом, ключ для механического замка и т.п.

1.3 Неотъемлемые свойства личности. Антропометрические характеристики человека, используемые для его идентификации. Наиболее известные примеры: отпечатки пальцев, отпечаток ладони, рисунок на сетчатке глаза, речевые признаки, элементы лица.

2. Многофакторная авторизация

Основным недостатком всех видов однофакторной авторизации, за исключением биометрической, является то, что элемент, на основании которого предоставляется доступ, может быть добровольно или насильственно передан другому лицу. Пароль можно случайно («записал на бумажке и потерял») или специально передать злоумышленнику, электронный или бумажный пропуск можно «одолжить» другому человеку, либо его могут отнять. Более того, не все биометрические признаки действительно являются «неотъемлемой частью человека». Если важность ресурса, к которому необходим несанкционированный доступ, очень велика, злоумышленники могут получить. Следовательно, для повышения надежности ограничения доступа рекомендуется использовать многоступенчатую систему авторизации, построенную на комбинации двух или более способов. Это может быть комбинация: пароль и отпечаток пальца, либо пароль и карта доступа.

Особенности использования речи для авторизации доступа

Главным преимуществом речи в системах биометрической верификации является то, что, в отличие от постоянных признаков человека, которые он не может произвольно менять, он может по своему усмотрению управлять тем, что он говорит. То есть, решение о допуске может приниматься не только на основании уникальных для каждого человека признаков голоса, но и на основании анализа произнесенной парольной фразе, интонации речи. Например, возможна такая, достаточно простая, схема: для каждого дня недели записывается свой речевой пароль. При этом:

- Идентификация пользователя по голосу является текстозависимой (даже без перевода речи в текст);
- Обеспечивается сразу два вида авторизации: человек знает необходимое слово и несет в себе необходимые для авторизации характеристики.

Другим неоспоримым достоинством использования речи в качестве биометрического признака является возможность верификации личности по признаку ее эмоционального состояния. Допустим, если человека заставляют произнести парольную фразу «под дулом пистолета», его голос, помимо воли (либо сознательно) изменяется. Этот факт можно использовать как основание для отказа в доступе на охраняемый объект, так и для определения того, что парольная фраза говорится под принуждением. Можно возразить, что это преимущество будет одновременно и недостатком системы биометрической верификации на основе речи, поскольку потенциально приводит к относительно высокому проценту «отказа своему». Однако, этот недостаток достаточно легко преодолевается с помощью самотренировки человека, и использования адаптивных алгоритмов верификации, которые отслеживают не-

большие изменения в характеристиках голоса. В разряд достоинств голосовой биометрической верификации можно смело отнести минимальные затраты на ее эксплуатацию. Системы с ее использованием не требуют установки сложного дорогостоящего оборудования, такого как считыватели отпечатков пальцев или радужной оболочки.

Еще одним недостатком верификации с помощью речи многие считают возможность использования аудиозаписей для получения несанкционированного доступа. Однако не нужно забывать, что биометрические признаки, используемые для верификации, в значительной степени зависят от особенностей речевого аппарата конкретного человека и искажаются при использовании технических средств, как на этапе записи, так и на этапе воспроизведения. Использование записи также не принесет «положительного» результата, в случае правильного подбора зависимости парольных фраз от внешних условий.

Например, можно построить систему авторизации таким образом, чтобы пользователь произносил название дня недели и цвета, изображенного на экране. Цвет отображается генератором случайных чисел из трех возможных, что дает 21 парольную фразу. В такой ситуации злоумышленник должен не только записать аудиосигнал нужного лица, но и знать алгоритм его использования. Такой подход позволяет создать бесконечное множество подобных легкозапоминаемых схем верификации [1].

Перед нами была поставлена задача разработки системы авторизации по голосу. После анализа существующих средств общая задача была разделена на две части: разработка макета аппаратной части системы авторизации по голосу и исследования алгоритмов авторизации. Первая часть задачи решалась путём определения требований к аппаратной части и выбора технических средств для ее реализации. В процессе рассмотрения разнообразных технических средств наш выбор остановился на относительно простом сигнальном процессоре dsPIC фирмы Microchip. Сигнальный процессор dsPIC имеет небольшое количество команд, что снижает порог вхождения в его программирование, а также обеспечивает необходимую скорость оцифровки сигнала (200 тысяч измерений в секунду)[2]. Основная задача аппаратной части это быстрая оцифровка звукового сигнала и передача этой последовательности персональному компьютеру. Среди дополнительных задач будет усиление сигнала, полосовая фильтрация, так как человеческий голос имеет ограниченную полосу частот (от 300 Гц до 4000 Гц) [3] и лишние гармоники будут мешать анализу. Основная часть задачи авторизации будет решаться в персональном компьютере, а аппаратная часть в дальнейшем выступит в качестве инструмента для изучения алгоритмов авторизации и будет выполнена в виде макета.

Вторая часть задачи решалась путем выбора программных средств, алгоритмов авторизации и способов их реализации с помощью выбранных программных средств. После рассмотрения различных программных средств

наш выбор остановился на среде программирования LabVIEW фирмы National Instruments которая объединяет простоту графического программирования с гибкостью мощного языка программирования. Использование среды LabVIEW позволяет упростить написание программного кода, так как использует специфичный язык графического программирования G, который можно освоить, не будучи программистом, но в то же время является полноценным компилятором и позволяет создавать исполняемые файлы (.exe).

Структурная схема системы авторизации представлена на рисунке.

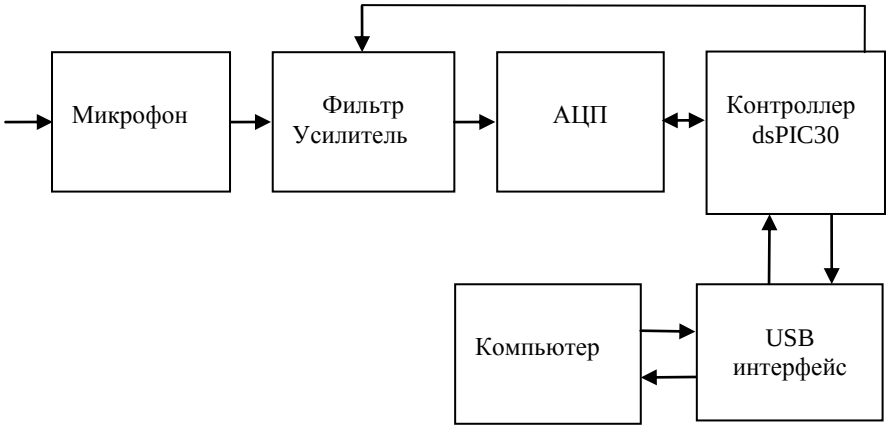

Рис. Структура системы авторизации

Виртуальная (программная) часть системы авторизации, расположенная в персональном компьютере, взаимодействует с аппаратной частью через высокоскоростной интерфейс. Разделение аппаратной и программной частей на два модуля позволяет вносить произвольные изменения в программную часть (модернизация и модификация) без изменения в аппаратной части, что позволяет быстро и эффективно менять характеристики системы авторизации, алгоритмы, применяемые в процессе работы системы.

Список литературы: 1. Перспективы использования речи для авторизации пользователей в системах разграничения доступа. Материал с сайта компании «Речевые технологии» **2.** dsPIC30F Family Overview Microchip Technology Inc. 2005. – 24 с. **3.** *Фролов Г. В.* Синтез и распознавание речи. Современные решения / Г. В. Фролов, С. М. Фролов. – 2008.

Поступила в редколлегию 06.10.11