УДК 57.087.1:621.391.26

ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СИСТЕМ ГОЛОСОВОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

О.Н. ФАЙЗУЛАЕВА[1], И.Ш. НЕВЛЮДОВ[2]

[1]Харьковский национальный университет радиоэлектроники
пр-т Ленина, 14, г. Харьков, 61166, Украина
olga_kharkov_2014@mail.ru

[2]Харьковский национальный университет радиоэлектроники
пр-т Ленина, 14, г. Харьков, 61166, Украина
tapr@kture.kharkov.ua

В работе предложены пути повышения качественных характеристик систем голосовой аутентификации пользователей, которые ориентированы на совершенствование системы ввода и выделения акустического сигнала. Представлены результаты имитационного моделирования предложенной системы ввода и выделения сигналов в процессе цифровой обработки регистрируемых сигналов. Предложенные решения позволяют повысить отношение сигнал/шум регистрируемых полезных сигналов.

Ключевые слова: аутентификация, биометрия, диаграмма направленности, голосовой сигнал, квадратурная обработка, микрофон, решетка.

Преступления в сфере информационных технологий (взлом паролей, кража номеров кредитных карточек и других банковских реквизитов) с каждым годом приобретают все больший размах. Согласно оценкам комиссии по внутренним делам британского парламента, годовые потери мировой экономики от этих преступлений достигли 388 млрд. долларов, что на 100 млрд. долларов превышает мировой оборот наркорынка. Особо обострилась эта проблема со стремительным внедрением веб-доступа к различным ресурсам и средствам, который создает потенциальные проблемы безопасности. Недостатки современных систем аутентификации пользователей в текоммуникационных системах и сетях приводят и к другим противоправным действиям, которые по оценкам специалистов лаборатории Касперского могут привести к «смерти Интернета», как глобальной информационной системы, уже в 2014 году.

В связи с этим ряд государственных и частных организаций выделяют большие средства и проводят интенсивные исследования в области усовершенствования систем аутентификации. При этом особое внимание уделяется биометрическим системам аутентификации. Биометрия принадлежит к тем областям современных технологий, темп развития которых стремительно увеличился после драматических событий 11 сентября 2001 года в Нью-Йорке.

Биометрические системы безопасности – это автоматизированные методы и средства идентификации личности посредством измерения уникальных физиологических особенностей или поведенческих характеристик человека и их сравнения с эталонами, хранящимися в соответствующих базах данных.

Первоначально основные усилия по решению стран «восьмерки» были сосредоточены на дактилоскопии (распознавание отпечатков пальцев), распознавании геометрии лица и радужной оболочки глаза. Эти идентификаторы рекомендовано использовать и при изготовлении биометрических паспортов.

В основу работы биометрических систем положена математическая статистика (а именно, проверка гипотез [1]), алгоритмы которой интенсивно используются в ряде

современных технических систем, таких как: связь, радиолокация (различные радары), множестве байесовских систем. В качестве двух основных характеристик такой системы, построенной на основе статистической теории проверки гипотез (тестов), можно принять ошибки первого и второго рода [1,2]. В теории радиолокации их обычно называют «пропуск цели» и «ложная тревога», а в биометрии, наиболее устоявшиеся понятия – FRR (False Rejection Rate, ложный отказ) и FAR (False Acceptance Rate, ложное распознавание). Первое число характеризует вероятность отказа доступа человеку, имеющему допуск. Второе – вероятность ложного совпадения биометрических характеристик двух людей.

Система тем лучше, чем меньше значение FAR при одинаковых значениях FRR. Здесь же заметим, что ошибки первого и второго рода в системах биометрической аутентификации приводят к различным последствиям, особенно для финансовых организаций [3]. К сожалению, современные биометрические системы, базирующиеся на физиологических особенностях пользователя, имеют низкие качественные характеристики и могут быть подделаны. Пользу указанные системы могут приносить в криминалистике или в антитеррористической деятельности. Поэтому в последнее время исследователи уделяют большое внимание поведенческим характеристикам пользователя и, в первую очередь, голосовой аутентификации.

В докладе анализируются преимущества систем голосовой аутентификации, которые позволяют иметь более высокую эффективность по отношению к системам на основе физиологических признаков пользователя. При этом существует актуальная научная задача повышения эффективности систем голосовой аутентификация.

Объектом исследования является процесс голосовой аутентификации в телекоммуникационных системах и сетях.

Целью данной работы является анализ основных путей, ориентированных на повышение качественных характеристик систем голосовой аутентификации.

На основе опыта разработки и применения различных радиолокационных средств и систем радиосвязи, обосновываются пути повышения эффективности систем голосовой аутентификации на основе:

- использования двух микрофонов и пространственно-временной обработки материалов регистрации;

- оптимизации расстояния между микрофонами с учетом длины регистрируемых волн (от 100 Гц до 8 кГц), формы диаграммы направленности двухэлементной решетки и размеров мобильных гаджетов;

- уточнения требований к частоте временной дискретизации регистрируемых колебаний с учетом обеспечения качественной цифровой обработки;

- детализации структурной схемы ввода и выделения голосового сигнала, за счет применения квадратурной обработки материалов регистрации и использования адаптивной схемы формирования весовых коэффициентов.

Приводятся и анализируются результаты имитационного моделирования.

Список литературы

1. *Гмурман В.Е.* Теория вероятностей и математическая статистика. М.: Высш. шк., 1999.

2. Теоретические основы радиолокации / Под ред. Я.Д. Ширмана. М.: Сов. радио. 1970.

3. *Пастушенко О.Н., Невлюдов И.Ш.* Анализ качественных показателей биометрических систем аутентификации пользователей / Электронное научное специализированное издание – журнал «Проблемы телекоммуникаций». 2012. № 4(9). С. 96-103.