аутентификации. Для реализации описанной функциональности может использоваться библиотека pocketsphinx.js. Библиотека разработана с использованием языка javascript и позволяет осуществлять распознавание речи в реальном времени прямо в браузере конечного пользователя. Принцип работы распознавания основан на использовании скрытых марковских моделей. Основные преимущества такого подхода – высокая скорость и точность распознавания. Для хранения эталонных образцов может осуществляться генерация словарей, на основании которых можно осуществлять аутентификацию пользователя по голосу.

Литература

1. Speech Silicon: An FPGA Architecture for Real-Time Hidden Markov-Model-Based Speech Recognition / J. Schuster [et al.] // J. Embedded Systems. 2006.

2. On Preprocessing of Speech Signals / A. Keerio [et al.] // International Journal of Signal Processing. 2009. № 5.

ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В МЕДИЦИНСКИХ СИСТЕМАХ

А.В. Курочкин, Е.А. Головатая

Внедрение информационных технологий в медицине обуславливает необходимость уделять значительное внимание вопросам информационной безопасности в различных видах систем медицинского учета. Конфиденциальность личных данных и защита информации, представляющей врачебную тайну, является важнейшей составляющей медицинских систем. Таким образом, при их проектировании необходима разработка комплексного решения по обеспечению конфиденциальности, целостности и доступности обрабатываемых данных.

Обеспечение конфиденциальности в медицинских системах осуществляется при помощи жесткого разграничения доступа к информации, представляющей врачебную тайну – электронным медицинским картам, историям болезни и т.п. Введение политики аудита обрабатываемых данных позволяет отследить возможные источники утечки информации. Использование процедур многофакторной аутентификации и введение политики смены парольной информации для персонала позволяет снизить риск несанкционированного доступа. При ограничении доступа необходимо учитывать, что конфиденциальными являются не только единичные записи, но и различные виды отчетной, сводной и статистической информации.

Для предотвращения угроз доступности информации необходимо исключить возможность доступа ко всей базе данных медицинских записей целиком, а также ограничить доступность внутренней сети медицинского учреждения извне. Кроме того, для предотвращения возможных последствий, можно использовать процедуру планового резервного копирования информации с физическим ограничением доступа к резервным копиям. Угрозы доступности данных в медицинских системах обычно стоят не так остро, как в системах с массовым доступом. Тем не менее, для снижения рисков ограничения доступности по непредвиденным обстоятельствам можно использовать репликацию или шардинг информации.

Литература

1. Гатчин Ю.А. Теория информационной безопасности и методология защиты информации / Ю.А. Гатчин, В.В. Сухостат. – СПб.: СПбГУ ИТМО, 2010. – 98 с.

2. Prater V.S. Confidentiality, privacy and security of health information: Balancing interests / V.S. Prater // University of Illinois, Chicago: Biomedical and Health Information Sciences, December 8, 2014.

АЛГОРИТМ ОБЕСПЕЧЕНИЯ СТРУКТУРНОЙ СКРЫТНОСТИ ИНФОРМАЦИОННОГО ПОТОКА НА ОСНОВЕ ШИРОКОПОЛОСНОГО СИГНАЛА

М.А. Лебедевич

В настоящее время к системам передачи информации предъявляются высокие требования к безопасности передаваемой по открытым каналам связи информации. Одним из основных путей обеспечения этих требований является использование сигналов с расширением