Целью данной работы является представление клиент-серверной системы, учитывающей особенности реализации формата JPEG, связанные с программно-технической реализацией цифровых фотокамер различных брендов и моделей, работа которой основана на применении методов машинного обучения для решения задачи определения цифровой фотокамеры (брэнд / модель), которой было сделано подлинное изображение, или определения графического редактора, которым были внесены изменения.

Сервис проверки подлинности цифровых изображений разработан и функционирует как локальное клиент-серверное приложение, так как передавать в локальную сеть, а тем более в сеть Интернет, криминалистически значимую информацию недопустимо. Сервис позволяет определять лишь подлинность изображений JPEG-формата, а сам процесс определения подлинности основан на алгоритмах классификации: построения дерева принятий решений и методе k ближайших соседей. В настоящее время база сервиса содержит информацию о 48 брендах (производителях цифровых фотокамер) и более чем 650 моделях.

СИСТЕМА SSO В ИНТЕГРИРОВАННОЙ СЕТИ

А.О. Качанова

Современная тенденция в области аутентификации является использование технологии единого входа (англ. Single Sign-On). Это удачный компромисс между безопасностью доступа к приложениям и удобством работы пользователя. Идея этой технологии заключается в обеспечении единой аутентификации для всех информационных систем организации, которые с точки зрения доступа являются разнородными и никак не интегрированы между собой или с общей службой каталогов. Кроме того, подобное решение повышает уровень информационной безопасности в части парольной политики. Областью практического применения данного исследования являются компании, которые имеют многочисленные внутренние подсистемы.

В докладе рассматривается система, использующая API технологию с использованием языка JSON, что позволяет обеспечить надежную политику безопасности, повышенную безопасность всех ресурсов предприятия, снизить вероятность возникновения критических ошибок, упростить процесс аутентификации пользователя в интегрированной сети. Система использует дополнительную биометрическую процедуру аутентификации.

Литература

1. Bashir, K., Asif, S. Important Considerations for Single Sign-On Solution. International Journal of Multidisciplinary Sciences and Engineering, 2010.

2. Bishop, M. Introduction to Computer Security. Boston: Pearson Education, 2005

АНАЛИЗ РЕЧЕВОЙ ИНФОРМАЦИИ КАК ЭТАП МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ В СЕТИ ИНТЕРНЕТ

Е.В. Кисель, А.В. Курочкин

В настоящее время значительное внимание уделяется задаче идентификации и аутентификации личности на основании одного или нескольких биометрических признаков. Одним из перспективных направлений в биометрической идентификации и аутентификации является распознавание речевой информации. Существенным преимуществом использования голоса в качестве одного из факторов аутентификации является отсутствие необходимости в сложном специализированном оборудовании – для записи образца голоса можно использовать обычный микрофон. Распознавание речевой информации может использоваться в качестве одного из факторов при проведении многофакторной аутентификации. В значительной степени многофакторная аутентификация может применяться для обеспечения безопасности при доступе на различные интернет-ресурсы. В данном контексте большой значимостью обладает задача автоматизированного распознавания речи в реальном времени в рамках проведения многофакторной аутентификации на веб-сайт. Пользователю предлагается, в качестве одного из этапов аутентификации для входа на защищенную зону веб-сайта, произнести заранее записанный пароль, который в дальнейшем сверяется с эталоном во внутренней базе данных; на основании результата сверки принимается решение о подтверждении или отклонении

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