

Таким образом, в статье исследованы существующие проблемы настоящих систем документооборота. Для решения этих проблем в статье предложена модель работы СЭД на основе мультиагента в виде UML, которая позволяет оптимизировать скорость и безопасность при разработке СЭД.

## СПИСОК ЛИТЕРАТУРЫ:

1. Нгуен Д. Х., Камасев В. А., Кизим А. В. Многоагентная система для построения удостоверяющих центров // Городу Камышину – творческую молодежь (посвящается 15-летию Камышинского технол. ин-та (филиала) ВолгГТУ): матер. III регион. н.-практ. студ. конф., 22–23 апр. 2009 г. / ВолгГТУ, КТИ (филиал) ВолгГТУ. Камышин, 2009. Т. 2. С. 75–78.

*Е. Е. Цицулин, А. П. Дураковский*

## АУТЕНТИФИКАЦИЯ ПО ГОЛОСУ: КОНТАКТНО-РАЗНОСТНЫЙ МЕТОД

В настоящее время аутентификация личности по голосу широко применяется в системах контроля доступа к информационным или материальным ресурсам на основе биометрических параметров. Системы аутентификации личности по голосу обладают рядом преимуществ относительно других биометрических систем, основными из которых являются сравнительно небольшая стоимость и относительная простота практической реализации [1].

Развитие систем аутентификации личности по голосу лимитируется уровнем их надежности. Точность идентификации (установление) и верификации (подтверждение) личности по голосу в существенной мере определяется адекватностью математической модели, описывающей речевой сигнал. Увеличение точности в рамках существующих методов описания речевых сигналов если и возможно, то приводит, как правило, к значительному увеличению количества параметров модели, что влечет за собой увеличение систематической ошибки и времени обработки поступивших данных, а также снижение значимости таких параметров для характеристики индивидуальных особенностей голоса человека. Высокий уровень ошибок систем аутентификации по голосу обуславливается также трансформацией голоса вследствие болезней, особых эмоциональных состояний, возрастных изменений и т. д. [1].

Существуют несколько методов синтеза и анализа математических моделей речевого сигнала. Они основываются на теории модуляции с использованием детерминированного подхода и стохастического подхода.

Голосовые системы аутентификации можно классифицировать по следующим признакам [1]:

1. Системы идентификации и верификации;
2. Системы индивидуальной и групповой идентификации;
3. Текстозависимые и текстонезависимые системы аутентификации;
4. Автоматические и экспертные системы.

Одним из существенных недостатков известных систем идентификации и верификации по голосу является трудность сохранения в тайне речевого сигнала как биометрического образа, а также малая степень защиты от имитации голоса с помощью различных звуковоспроизводящих устройств. Это обусловлено тем, что речевой сигнал представляет собой изменения давления воздушной среды его распространения, формируемые речевым трактом человека. Использование



современных звукозаписывающих и звуковоспроизводящих устройств позволяет злоумышленнику фальсифицировать в процедурах аутентификации биометрический образ зарегистрированного в системе пользователя [2].

Развитием идентификации личности по голосу является контактно-разностный метод, использующий акустические характеристики человеческого тела в качестве биометрического параметра для идентификации. При этом акустическую модель тела человека можно представить в виде сложной уникальной системы проводников звукового сигнала, формируемого в носоглотке человека при произнесении каких-либо звуков. Использование специальных датчиков ларингофонного типа позволяет регистрировать звуковые сигналы, распространяющиеся через биологические жидкости, мягкие и твердые ткани человека, с последующим формированием индивидуального биометрического образа. При идентификации сигналы снимаются с выбранной области регистрации колебаний — это может быть, например, голова, плечо, локоть, запястье руки, колено и т. п. Следует отметить, что для различных точек наблюдения (областей регистрации) сигнала, вследствие разных трактов звукопередачи, акустические характеристики принимаемых колебаний будут отличаться. Таким образом, если злоумышленник не знает область регистрации акустического сигнала, то фальсификация такого принимаемого колебания существенно усложняется [2].

## СПИСОК ЛИТЕРАТУРЫ:

1. Голубинский А. Н., Булгаков О. М. Система аутентификации личности по голосу на основе математической модели речевого сигнала // XXIII Международная научная конференция «Математические методы в технике и технологиях»: Сборник трудов. Т. 6. Саратов, 2010. С. 19–22.
2. Голубинский А. Н., Дворянkin С. В. Обработка акустических сигналов при контактно-разностном методе идентификации личности // Безопасность информационных технологий. 2011. № 3. С. 10–16.

Д. С. Чернявский

## УНИФИКАЦИЯ ПРАВИЛ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕВЫХ СРЕДСТВ ЗАЩИТЫ

Для повышения эффективности разработки и реализации политики информационной безопасности (ИБ) необходимо унифицировать способ задания правил политики и процесс настройки сетевых средств защиты (ССЗ) [1]. Предлагаемым решением является унифицированный язык правил политики ИБ ССЗ [2] (далее — унифицированный язык), который позволяет задавать и реализовывать правила политики ИБ независимо от пользовательских интерфейсов и внутреннего устройства конкретных ССЗ.

В общем случае правило политики ИБ, формализованное с использованием унифицированного языка, имеет следующий синтаксис:

$Identifier\ action\ function1(param11 \dots param1N) \dots functionK(paramK1 \dots paramKM)$ ,  
здесь *identifier* — некоторый идентификатор правила, *action* — действие,  $Function1 \dots functionK$  ( $K \in \mathbb{N}$ ) — функции безопасности, выполняемые ССЗ, с параметрами  $param11 \dots param1N$ ,  $paramK1 \dots paramKM$  ( $N, M \in \mathbb{N}_0$ ). Порядок и структура параметров зависят от конкретной функции. На данный момент унифицированный язык поддерживает формализацию функций

