Владимир Темников, Елена Темникова*
*Национальный авиационный університет, *Национальный технический университет Украины «Киевский политехнический институт»*
УДК 004.931

КОНЦЕПЦИИ ПОСТРОЕНИЯ ГОЛОСОВЫХ СИСТЕМ КОНТРОЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ ДЛЯ РАЗЛИЧНЫХ УСЛОВИЙ ПРИМЕНЕНИЯ

Анотация: **Предложены концепции построения голосовых систем контроля доступа к информационным ресурсам для двух вариантов применения систем в зависимости от специфических особенностей, обуславливающих требования к этим системам. Для каждого варианта описаны подсистемы и составляющие их модули, изложены принципы функционирования модулей в зависимости от условий, характеризующих область применения.**
Summary: **In the article proposed the concept of building systems of access control to information resources by voice for the two applications systems of access control depending on the specific characteristics causing the requirements for these systems. Subsystems and components of modules are described, the principles of operation of modules depending on the characterizing area of application for each variant are presented.**
Ключевые слова: **Аутентификация, идентификация, контроль эмоционального состояния.**

I Введение

Наиболее значимыми в настоящее время задачами, связанными с обеспечением автоматизированного контроля доступа людей к ресурсам информационных систем по голосу, являются:

1. в банковской и информационно-справочной областях – контроль удаленного доступа абонентов к информационным ресурсам банковских, справочных и других подобного рода информационных систем (например, при управлении клиентом банка его банковским счетом, при получении абонентом сведений справочного характера) с применением мобильного или стационарного телефона, смартфона или другого аналогичного устройства; круглосуточный доступ к информации обеспечивает оперативность и удобство при активной деловой и научной деятельности.

2. на транспорте, в энергетике и других отраслях, где используется операторский труд – перманентный контроль доступа операторов (авиадиспетчеров, операторов энергетических систем и др.) к информационным ресурсам эргатических систем в процессе выполнения ими своих функциональных обязанностей; безопасность на транспорте и в энергетике существенно зависит от правильности действий операторов, ошибки в работе которых могут быть вызваны испытываемым ими нервно-эмоциональным напряжением, при этом использование голоса оператора в качестве анализируемого образа дает возможность осуществлять контроль бесконтактно, дистанционно, не отвлекая оператора от работы.

Каждый из этих вариантов применения систем контроля доступа (СКД) имеет свои специфические особенности, которые обусловливают требования к этим системам.

Особенностями первого из обозначенных применений СКД (применение систем контроля доступа абонентов к ресурсам банковских и справочных информационных систем) являются необходимость использования проводной или беспроводной связи, вызванная значительным расстоянием между абонентом и СКД, и большое количество контролируемых лиц (абонентов – клиентов банков или справочных информационных систем). Указанные особенности применения обусловливают предъявление повышенных требований к системам шумоподавления и необходимость учета наличия большого количества эталонов в базах данных (БД) СКД**.** Применяемые в настоящее время в банковской и справочной сферах СКД обычно выполняют лишь аутентификацию абонентов по парольным фразам – система в процессе диалога между ней и абонентом просит человека произнести определенный набор слов.

Особенностями второго из обозначенных применений СКД (применение систем контроля доступа операторов к информационным ресурсам эргатических систем) являются незначительные шумы анализируемого речевого сигнала, что связано с малым расстоянием от источника звука до СКД, и небольшое количество контролируемых лиц, обусловливающее относительно малое количество эталонов в БД. Другими, специфическими для контроля операторов (в первую очередь – авиадиспетчеров), особенностями применения СКД являются использование специальной нормативно установленной фразеологии, а также выдвигаемые нормативными документами требования по размеренности речи и неизменности расстояния между авиадиспетчером и микрофоном.

Указанные особенности применения обусловливают предъявление повышенных требований к

быстродействию систем (необходимо обеспечить работу СКД в режиме реального времени) и относительную сложность СКД, связанную с необходимостью обеспечения текстонезависимого распознавания оператора.

В настоящее время в процессе проведения допуска операторов к их рабочим местам проводятся лишь предсменный медицинский контроль и визуальный контроль на рабочем месте.

В статье на основе анализа особенностей применения СКД разработаны концепции их построения для указанных выше условий применения.

Внедрение концепции построения систем контроля удаленного доступа абонентов к информационным ресурсам банков позволит обеспечить значительное повышение функциональности СКД по сравнению с существующими за счет дополнительного проведения контроля эмоционального состояния (ЭмС) абонента, а также идентификации абонентов на предмет их отсутствия в «черных списках» и выявления мошенников.

Разработка концепции построения СКД для второго варианта их применения была нацелена на проведение аутентификации, контроля (мониторинга) ЭмС и идентификации (в случае непрохождения аутентификации) операторов по непрерывной речи, а также контроль степени утомления операторов по параметрам, характеризующим состояние сердечно-сосудистой системы (как интегрального показателя психофизиологического состояния человека) на основе совершенствования предсменного и введения внутрисменного (во время перерывов в работе) и послесменного психофизиологического контроля операторов.

II Концепция построения системы контроля удаленного доступа абонентов банков и справочных систем

В соответствии с разработанной концепцией, системы контроля удаленного доступа абонентов должны содержать в своем составе подсистемы аутентификации, контроля ЭмС и идентификации. Контроль при этом осуществляется по парольным фразам.

Подсистема аутентификации абонента

Голосовую подсистему аутентификации предлагается строить на основе теории распознавания образов [1]. При этом, особое внимание при разработке подсистемы, наряду с параметризацией и классификацией – основными составляющими процесса аутентификации, должно быть уделено шумоподавлению.

Модули параметризации и классификации

Концепция предусматривает совместную разработку модулей параметризации и классификации. Модуль параметризации при этом рекомендуется строить таким образом, чтобы обеспечить эффективную работу модуля классификации.

Модуль классификации абонентов предлагается строить на основе искусственных нейронных сетей (ИНС). При этом, к ИНС предъявляются следующие требования:

1. возможно меньшее количество применяемых информативных параметров, характеризующих речевые сигналы, при обусловленных значениях ошибок первого и второго рода (процента правильной аутентификации);
2. возможно меньшее необходимое время обучения при обеспечении заданного качества проведения аутентификации;
3. возможно более высокая скорость обработки речевых сигналов.

Исследования показали, что в качестве ИНС целесообразно применять многослойный перцептрон с одним скрытым слоем.

Параметризацию речевого сигнала предлагается проводить с применением метода кратковременного анализа [2]. В [3] на основе сравнительного анализа возможных вариантов выбора информативных параметров речевых сигналов было обосновано применение кепстральныхкоэффициентов линейного предсказания (ККЛП), рассчитанных на каждом фрейме, и приведен алгоритм их расчета.

Для удовлетворения требований, предъявляемых к параметрам речевых сигналов со стороны ИНС, совместно с Конфоровичем И. В. разработана система информативных параметров, построенная на основе пофреймово рассчитанных ККЛП [4].

Конкретные вид ИНС и значения параметров модулей параметризации и классификации речевых сигналов определяются в процессе совместного тестирования этих модулей по критерию максимума процента правильной аутентификации. Результаты тестирования, проведенного в процессе разработки системы контроля, приведены в [4].

Достигнутый в результате тестирования процент правильной аутентификации составил 98%.

Модуль шумоподавления

Высокий уровень шумов анализируемого речевого сигнала обусловливает использование систем

шумоподавления с повышенным уровнем очистки.

При решении задачи очистки речевого сигнала от шума и помех предлагается применять технологии вейвлет-преобразования данных [5-7], предусматривающие разложение речевого сигнала на аппроксимирующие коэффициенты, которые характеризуют сглаженный сигнал, и детализирующие коэффициенты, описывающие колебания [8]. В связи с тем, что шумовая компонента больше отражается в детализирующих коэффициентах, при удалении шума обрабатываются именно они.

В соответствии с разработанной методикой, шумоподавление предлагается проводить в среде MatLab в следующей последовательности.

1. Выбор вейвлета и уровня разложения N (до которого производится вейвлет-разложение исходного сигнала) зависит от свойств конкретного сигнала – более гладкие вейвлеты создают более гладкую аппроксимацию сигнала и, наоборот, „короткие" вейвлеты лучше отслеживают пики аппроксимируемой функции. Глубина разложения влияет на величину отфильтровываемых деталей.

В эксперименте для разложения исходного исследуемого сигнала применялись вейвлеты Хаара, дискретные аппроксимации вейвлетов Мейера, вейвлеты Добеши, симлеты и койфлеты при уровнях разложения N=1÷8.

2. Пороговая обработка детализирующих вейвлет-коэффициентов. Для каждого уровня от 1 до N выбирается порог и проводится мягкая пороговая обработка детализирующих коэффициентов.

От выбора порогового уровня шума (дисперсии шума) зависит качество шумоподавления сигнала, оцениваемое в виде отношения сигнал/шум. Задание малых значений порога сохраняет информацию о шумовой составляющей в коэффициентах детализации и поэтому приводит лишь к незначительному увеличению отношения сигнал/шум. При больших значениях порога можно потерять коэффициенты, которые несут существенную информацию. Поиск оптимального значения означает отыскание такого порога, который при наименьшем смещении восстановленного сигнала обеспечивает наибольшее значение отношения сигнал/шум.

Для выбора оптимального порогового значения в эксперименте использовались адаптивный и эвристический критерии Штейна несмещенной оценки риска, универсальный и минимаксный критерии [6].

3. Вейвлет-реконструкция, основанная на первоначальных аппроксимирующих коэффициентах уровня N и модифицированных детализирующих коэффициентах уровней от 1 до N.

4. Сравнение очищенного сигнала с исходным сигналом путем расчета коэффициентов корреляции.

5. Выбор оптимальных характеристик шумоочистки (типа вейвлета, уровня его разложения, метода обработки) на основе анализа рассчитанных коэффициентов корреляции.

Подсистема контроля эмоционального состояния (ЭмС) абонента

Контроль ЭмС абонента по голосу позволяет в процессе дистанционного осуществления банковских операций (телефонного разговора) отслеживать изменение ЭмС абонента и прекращать разговор с абонентом в случае обнаружения неадекватности его поведения.

Контроль ЭмС предлагается проводить на основе сравнительного анализа контрольных и эталонных информативных параметров, характеризующих отдельные (в первую очередь гласные) фонемы.

В процессе разработки концепции были проведены теоретические и экспериментальные исследования, целью которых являлся анализ параметров, характеризующих речевые фрагменты, с точки зрения их эффективности для определения ЭмС. Исследования показали, что в качестве информативных параметров целесообразно использовать частоты основного тона, параметры, рассчитанные на их основе (в частности, изрезанность), формантные частоты гласных фонем, а также продолжительность произнесения абонентом речевых фрагментов. Исследования подтвердили имеющуюся в литературе информацию, что значения частот основного тона имеют довольно четкую тенденцию к повышению при изменении ЭмС человека по линии «депрессия, скованность – норма – возбуждение».

Сегментацию на фонемы предлагается, как и шумоподавление, проводить с применением вейвлетов.

Задача сегментации посредством вейвлетов решается путем обнаружения межфонемных переходов, на которых сигнал претерпевает значительные изменения одновременно на многих масштабах исследования и, соответственно, характеризуется возрастанием вейвлет-коэффициентов для многих уровней детализации, в то время как на стационарных участках фонем вейвлет-коэффициенты оказываются сгруппированными вблизи определенных масштабов. Поиск межфонемных границ сводится к поиску моментов увеличения вейвлет-коэффициентов на значительном количестве уровней масштабирования. Существенным является выбор вейвлетного базиса, который должен позволять описывать стационарный речевой сигнал со сравнительно малым числом ненулевых коэффициентов. Целесообразным для решения поставленной задачи в качестве вейвлет-базиса использовать вейвлеты Хаара-5 или Добеши-6.

Важным при определении ЭмС абонентов является отсутствие необходимости в распознавании всех фонем парольного речевого фрагмента – для определения ЭмС абонента достаточно распознать лишь несколько первых гласных фонем.

Подсистема идентификации абонента

Идентификация является необходимой при непрохождении контролируемым лицом процедуры аутентификации. Процедура идентификации также может быть затребована для борьбы с мошенничеством (путем сравнения голоса абонента с некоторым списком потенциальных мошенников).

Задача идентификации в данном случае значительно усложняется в связи с большим количеством контролируемых лиц и связанным с этим большим количеством эталонов в БД – в отличие от аутентификации, идентификация абонента требует большого количества расчетов для определения расстояний между тестовыми (контрольными) векторами параметров и векторами параметров, составляющими модели абонентов в БД.

Повышения скорости идентификации (при небольшом увеличениии процента неправильной идентификации) можно добиться путем устранения областей «молчания» в речевом потоке, применения «закрытой» идентификации, в процессе которой принимается решение о том, кто из зарегистрированных пользователей наиболее похож на автора тестируемого образца, разработки новых алгоритмов для быстрого поиска в метрических пространствах.

Авторами разработана процедура ускорения процесса идентификации, основанная на методах кластерного анализа. Идея процедуры заключается в кластеризации моделей абонентов в БД и перманентном (в режиме реального времени) уменьшении количества представляемых для сравнения моделей абонентов (кластеров) из БД путем исключения тех моделей (кластеров), к которым наименее вероятно принадлежит идентифицируемый образец (голос или изображение). Указанная процедура проводится неоднократно по мере поступления (в режиме реального времени) для анализа очередного вектора параметров тестируемого образца, и продолжается до тех пор, пока не останется один или несколько кластеров.

III Концепция построения системы контроля доступа операторов

В настоящем разделе представлены принципы построения основных подсистем системы голосового контроля за действиями операторов, обеспечивающей проведение перманентных аутентификации (для предотвращения доступа к информационным ресурсам несанкционированных лиц), идентификации (в случае непрохождения аутентификации) и мониторинга ЭмС операторов (для предотвращения доступа лиц, находящихся в ненадлежащем ЭмС) по непрерывной речи оператора.

Основными подсистемами СКД в соответствии с разработанной концепцией являются подсистемы аутентификации, мониторинга ЭмС и идентификации оператора по непрерывной речи оператора, а также распознавания ключевых слов в непрерывной речи.

Подсистемы аутентификации и мониторинга ЭмС операторов

Аутентификация и мониторинг ЭмС по непрерывной речи сводятся к аутентификации и мониторингу ЭмС по ключевым словам, выделенным из непрерывной слитной речи оператора. В качестве ключевых могут быть выбраны слова, часто употребляемые операторами в процессе работы или взятые из профессиональной фразеологии (это в первую очередь относится к авиадиспетчерам, для которых профессиональная фразеология установлена нормативными документами). Работа подсистем аутентификации и мониторинга ЭмС по ключевым словам аналогична работе подсистем аутентификации и мониторинга ЭмС по парольным словам, описанным в разделе II. Заметим, что модуль шумоподавления может быть построен по более простой схеме, чем это предлагалось в разделе II.

Особенностью задачи контроля за действиями операторов является возможность контроля степени утомления, сонливости и тревоги оператора на всех этапах его рабочей смены, начиная с предсменного медицинского контроля и заканчивая послесменным контролем. Об указанных состояниях оператора и их развитии в течение рабочей смены можно судить на основе результатов анализа состояния сердечно-сосудистой системы оператора (последнее является интегральным показателем состояния человека) по параметрам, характеризующим вариативность сердечного ритма [9, 10]. Определять эти параметры необходимо в процессе пред- и послесменного психофизиологического контроля оператора, а также в перерывах в его работе, с применением портативных электрокардиографов [11].

Подсистема идентификации операторов

Для ускорения поиска нарушителя режима доступа (если такой выявится в процессе аутентификации) в разработанной СКД, ввиду малого количества контролируемых лиц, вместо последовательного проведения аутентификации и идентификации предлагается сразу проводить идентификацию операторов. Для этого подсистема идентификации строится на основе ИНС с несколькими выходами. Результатом расчетов является вектор размерности n, каждый (i-ый) элемент которого является вероятностным значением того, что

поступивший на вход ИНС речевой сигнал принадлежит і-му оператору. Естественно, при этом усложняется процесс обучения ИНС.

В процессе идентификации параметризация и классификация речевых сигналов осуществляются аналогично тому, как это предлагалось делать при аутентификации.

Подсистема поиска ключевых слов в непрерывной речи оператора

Для поиска ключевых слов в непрерывной слитной речи оператора предлагается применять дикторонезависимые ИНС, обученные на распознавание ключевых слов. Применение ИНС позволяет существенно повысить точность работы СКД по сравнению с другими системами, работа которых основана на определении расстояний между контрольными и эталонными (занесенными в БД) векторами параметров.

Очевидно, что простой перебор слов при использовании ИНС является непродуктивным. Повышение быстродействия работы системы может быть достигнуто путем быстрого отбрасывания слов, заведомо не входящих в состав БД (словарь) ключевых слов перед их обработкой подсистемой аутентификации. В этом случае применение ИНС необходимо лишь для проверки гипотез, полученных в процессе применения разработанного способа.

Значащим этапом при применении разработанного способа повышения быстродействия работы системы является составление моделей слов, выделенных из непрерывной речи оператора. Указанные модели представляют собой последовательности позиций, предназначенных для распознанных фонем; при этом, под распознаванием понимается как собственно распознавание фонем (в первую очередь, гласных), так и отнесение фонемы к определенному классу (например, классу глухих согласных).

База моделей слов (БМС) создается на этапе регистрации операторов. При применении разработанного способа отбрасываются слова, модели которых не соответствуют моделям слов, составляющим БМС. Важным является отсутствие необходимости распознавания всех фонем ключевого слова – достаточно распознать (или отнести к определенному классу) несколько фонем – их последовательность составит гипотезу, подтверждаемую или отбрасываемую ИНС.

Таким образом, реализация разработанного способа повышения быстродействия работы системы заключается в выполнении следующей последовательности действий.

1. Составление модели контрольного ключевого слова, построенной по первым распознанным фонемам слова.
2. Поиск в БМС модели, соответствующей слову, поступившему для анализа. В случае наличия в БМС соответствующей модели выдвигается гипотеза, что анализируемое слово есть в словаре.
3. Проверка гипотезы с применением ИНС.
4. При «положительном» исходе проверки гипотезы переходим к проведению аутентификации оператора.

Заметим, что применение разработанного способа не требует дополнительных затрат времени, т. к. сегментация на фонемы и распознавание гласных фонем являются элементами последовательности действий, совершаемых во время проведения мониторинга ЭмС операторов.

IV Выводы

В статье предложены концепции построения двух типов голосовых систем контроля доступа (СКД) к информационным ресурсам, которые предназначены для применения в двух различных условиях. Каждое из этих условий применения обладает своими специфическими особенностями, которые обусловливают требования к системам каждого типа.

Первый тип СКД – это системы контроля доступа абонентов к ресурсам банковских и справочных информационных систем, характеризующиеся значительными расстояниями от абонентов до СКД, что обусловливает наличие в анализируемых речевых сигналах значительных шумов (помех), и большим количеством контролируемых лиц. Второй тип СКД – это системы контроля доступа операторов к информационным ресурсам эргатических систем, характеризующиеся небольшим расстоянием от источника звука до СКД, относительно незначительными шумами, малым количеством контролируемых лиц, спецификой работы операторов (требованиями к применению определенной нормативно установленной фразеологии, размеренности речи и др.).

Для каждого типа СКД приведены предложения по составу и построению подсистем.

Сочетание различных методов и подходов к построению подсистем СКД (методов вейвлет-преобразований, кепстрального анализа, кластеризации и др.), применение искусственных нейронных сетей и алгоритмов, основанных на метриках, позволяет создать системы контроля доступа, имеющие более высокие точность и быстродействие по сравнению с существующими системами, для применения в различных конкретных условиях эксплуатации.

Список использованной литературы: ***1.*** *Рамишвили Г. С. Автоматическое опознавание говорящего по голосу. // М.: Радио и связь, 1981. – 224 с.* ***2.*** *Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов. // М: Мир, 1978. – 848 с.* ***3.*** *Темников В. А., Шарий Т. В., Темникова Е. Л., Конфорович И. В. Голосовая аутентификация операторов, использующих в процессе работы нормативно установленную фразеологию // Інформаційна безпека. – 2011. – №1(5). – С.125-130.* ***4.*** *Темников В. А., Темникова Е. Л., Конфорович И. В. Выбор параметров системы аутентификации человека по голосу // Інформаційна безпека. – 2012.– №2(8). – С.151-157.* ***5.*** *Donoho, D. L. De-Noising by soft-thresholding // IEEE Trans. on Inform. Theory. - Vol.41. - №3. - 1995. - P.613-627.* ***6.*** *Смоленцев Н. К. Основы теории вейвлетов. – М.: ДМК, 2005. − 303 с.* ***7.*** *Темников В. А., Пономаренко Л. В. Методика проведения шумоочистки речевого сигнала в процессе распознавания // Вестник Восточноукраинского национального университета им. В. Даля. - №5 (111). – Ч.1. – 2007. – С.123-127.* ***8.*** *Астафьева Н. М. Вейвлет-анализ: основы теории и примеры применения // Успехи физических наук. – 1996. – Т.166. – №11. – С. 1145-1170.* ***9.*** *Баевский Р. М. Анализ вариабельности сердечного ритма: история и философия, теория и практика // Клиническая информатика и телемедицина. - 2004. – №1.- С. 54-64.* ***10.*** *Кальниш В. В., Романенко Е. В., Самойлов В. Д. Архитектура системы и разработка программных средств автоматизации диагностики психологических и психофизиологических качеств оперативно-диспетчерского персонала. – К.: ИПМЭ, 1989. – 53 с.* ***11.*** *Темников В. А., Темникова Е. Л. Определение психофизиологического состояния оператора в системе автоматического внутрисменного мониторинга по голосу // Вестник Восточноукраинского ационального университета им. В. Даля. - №6 (136). – Ч.1. – 2009. – С.294-297.*

Сергей Малышкин
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

УДК 654.924

ПОДХОД К ОЦЕНКЕ ВЕРОЯТНОСТИ ОБНАРУЖЕНИЯ УГРОЗЫ ИНТЕГРИРОВАННОЙ СИСТЕМОЙ БЕЗОПАСНОСТИ

Аннотация: **Рассматривается модель объекта как совокупность множеств подсистем, угроз объекту и зон объекта. Анализируется суммарная вероятность обнаружения произвольной угрозы интегрированной системой безопасности с учетом вклада подсистем и зон объекта в обнаружение. Анализируется вероятность обнаружения нарушителя с учетом маршрута его проникновения.**
Summary: **The object model is considered as aggregate of a set of the subsystems, the threats and the zones. The total detection probability of a threat by the integrated security system is analyzed with regard to the contribution of the subsystems and the object zones to the detection. The intruder detection probability is analyzed with regard to their penetration route.**
Ключевые слова: **Система безопасности, вероятность обнаружения, угроза.**

I Введение

В настоящее время большое распространение получили интегрированные системы безопасности (ИСБ), подсистемы которых объединены каналами связи и имеют общие средства сбора и обработки информации и управления. Как основные достоинства таких систем обычно отмечаются повышение эффективности управления и сбора информации, проверка тревог (т. е. снижение вероятности ложных тревог) и др. И в меньшей степени учитывается возможность повышения вероятности обнаружения угроз за счет правильной организации взаимодействия (т. е. интеграции) между подсистемами ИСБ. Вследствие интеграции подсистем на том или ином уровне можно говорить об увеличении вероятности обнаружения (ВО) угроз по сравнению со случаем использования отдельных не взаимосвязанных подсистем. В общем случае вероятность обнаружения угрозы ИСБ в целом зависит от вероятностей обнаружения этой угрозы отдельными подсистемами. А вероятность обнаружения угрозы подсистемой, в свою очередь, зависит от параметров средств обнаружения (СО). Поэтому для анализа эффективности ИСБ в целом необходимо знать вклад отдельных СО в обнаружение угроз и, в частности, несанкционированного проникновения. Этим вопросам в отдельности посвящены ряд работ, например, [1 – 3]. Однако в них не рассматривается вопрос в совокупности с учетом специфики именно ИСБ. Поэтому целесообразно дать оценку вероятности обнаружения угрозы интегрированной системой безопасности с учетом возможности повышения вероятности обнаружения за счет интеграции подсистем ИСБ. Такая оценка может служить одним из критериев эффективности ИСБ.