

Таблица 2
Состояния выработок

Выработка	Датчик1		Датчик2		Датчик3		..	Состояние
	Мин	Макс	Мин	макс	мин	макс		
Выработка вент закл. Гор -620 м	0,4 %	0,5 %	20 °С	30 °С	5 м/с	3 м/с	..	Штатное
Выработка вент закл. Гор -620 м	0,5 %	0,6 %	Любое	Любое	Любое	Любое	..	Предава- рийное
Выработка вент закл. Гор -620 м	Любое	Любое	30 °С	50 °С	Любое	Любое	..	Тревожное
Выработка вент закл гор -580 м	0,3 %	0,5 %	20 °С	30 °С	3 м/с	5 м/с	..	Штатное
Выработка вент закл гор -580 м	0,5 %	0,6 %	Любое	любое	Любое	Любое	..	Предава- рийное

Предложенный подход к построению подсистемы план ликвидации аварий предназначен для интеграции ее в АСО-ДУ, с целью использования преимущества непрерывного мониторинга ситуации. Это

позволит снизить влияние человеческого фактора на вынесение управленческих решений и повысить безопасность работ под землей.

СПИСОК ЛИТЕРАТУРЫ

1. Методы прогнозирования экономических показателей. – М., Финансы и статистика, 1986.
2. Теория прогнозирования и принятия решений. – М.: Высшая школа, 1977.
3. Построение экспертных систем. – М.: Мир, 1987.

Коротко об авторах

Чудинов С.Г. – магистр,
Кубрин С.С. – доктор технических наук, профессор,
Ландер А.В. – кандидат технических наук, доцент,
Московский государственный горный университет.



© А.С. Жуков, К.Ю. Кутейников,

В последнее время все чаще стали появляться на слуху понятия "аутентификация" и "верификация". Для специалистов в области биометрии эти понятия не составляют труда. Но для нас, простых обывателей, сталкивающимися с ними почти каждый день (например, при работе с компьютером или при денежных операциях через банкомат), эти понятия совершенно не знакомы, что, безусловно, является большим минусом, так как в скором будущем, в рамках проекта "Электронная Россия", биометрические технологии прочно войдут в нашу жизнь, усовершенствовав методы идентификации личности. Эта необходимость вызвана тем, что при подтверждении личности путем ее сличения с фотографией в документе велика вероятность ошибок. Целью внедрения биометрической информации является необходимость более достоверной "привязки" личности субъекта к предъявляемому документу. Это позволит значительно уменьшить вероятность использования поддельных и недействительных документов, а также повысить общий уровень безопасности.

Что же касается аутентификации и верификации, то тут, если разобраться, все просто. Оба эти понятия происходят от идентификации. Идентификация – это одно или большее количество измерений биометрической характеристики со считывающего устройства, которые преобразуются в пригодную для использования цифровую форму и затем сравниваются:

- с единственным шаблоном, соответствующим проверяемому человеку. Шаблон выбирается по предварительно вводимому номеру или коду. Результаты сравнения возвращаются приложению – такая процедура называется верификацией или

сравнением "один к одному". Результатом сравнения обычно является число – вероятность того, что сравниваемые шаблоны принадлежат одному лицу. Затем, с использованием какого-либо математического критерия, принимается решение об идентичности шаблонов;

- со всеми зарегистрированными шаблонами (без предварительного выбора шаблона и ввода номера или кода). В качестве результата возвращается список нескольких наиболее похожих шаблонов (с наибольшими вероятностями, полученными при сравнении). Затем, как и в предыдущем случае, с использованием какого-либо математического критерия, принимается решение об идентичности шаблонов. Такая процедура называется аутентификацией или сравнением "один ко многим". Об этих понятиях можно говорить много и посветить им не один десяток статей, но сейчас не об этом. Поговорим о грядущем, о биометрии.

Очень скоро с помощью внедренных биометрических технологий будет проходить идентификация человека по уникальным для каждого биологическим особенностям. Основные, используемые в настоящее время биометрические параметры это: кисть руки, черты лица, термограмма лица, температурная карта лица, голос, подпись, радужная оболочка глаза, папиллярный узор пальца и фрагменты генетического кода. На основе этих характеристик существуют одноименные способы распознавания. Все они уникальны и универсальны.

Одним из простейших способов является распознавание по кисти руки, основанное на анализе трехмерного изображения кисти. На сегодняшний день данный способ достаточно широко распространен, но не очень надежен. Это связано, в первую очередь, с

большой вариабельностью формы кисти. Плюсом можно считать малый размер математического "описания" кисти (длина "описания" составляет примерно 10 байт).

Следующим по сложности и частоте использованию является метод распознавания черт лица. Данный способ основан на анализе большого количества параметров, таких как цвет, форма, контраст, черты и т.д. Системы подобного рода в настоящее время имеют недостаточную надежность распознавания из-за больших ограничений, связанных с освещенностью и ракурсом лица во время ввода параметров идентификации, но распространены достаточно широко (около 15 % рынка).

Распознавание по термограмме лица основано на результатах исследований, которые показали, что термограмма, т.е. схема расположения кровеносных сосудов лица (вены, артерии), является уникальной для каждого человека. Система позволяет провести идентификацию даже в случае, когда человек находится в другом конце неосвещенной комнаты. Такие факторы, как температура тела, охлаждение кожи лица в морозную погоду, естественное старение организма человека, использование специальных масок не влияют на точность термограммы. Однако и здесь есть свой минус – это высокая стоимость. Метод распознавания по температурной карте лица очень похож на распознавание по термограмме лица. Главным отличием является то, что в этом случае учитываются температурные особенности самой кожи лица, хотя они и зависят от расположения кровеносных сосудов. Уникальность и устойчивость метода пока еще недостаточно доказаны, но при определенных условиях он показывает отличные результаты.

Надежная идентификация человека по голосу пока остается неразрешимой проблемой. Хотя человеческое ухо и мозг являются наиболее совершенными инструментами идентификации, зачастую мы не узнаем голоса, которые слышим по телефону. Основная проблема заключается в большом разнообразии проявлений голоса человека:

он может меняться в зависимости от настроения, состояния здоровья, от возраста и т.д.

Идентификация человека по его подписи – достаточно надежный метод биометрической идентификации личности, однако процедуры распознавания пока слишком сложны и неудобны в применении. Представьте себе, что для получения доступа Вам придется расписываться привязанной ручкой на вмонтированном в стену, дверь или стол планшете. Возможно поэтому этот метод является пока экзотикой и не находит серьезного применения.

Идентификация по радужной оболочке глаза имеет высокую степень надежности, однако, соответствующие устройства ввода изображения радужной оболочки глаза имеют пока довольно высокую стоимость. Вдобавок – существуют проблемы, связанные с процедурой сканирования. Устройство сканирования, фактически, является высококачественной телекамерой, что определяет некоторые неудобства, связанные с размером камеры и собственно процедурой сканирования.

Сейчас же наиболее часто используемый метод – это распознавание папиллярного узора пальца. Проверка отпечатков пальцев проходит на основе анализа и сравнения папиллярных узоров. При сравнении соответствующих процедур идентификации по надежности метод сопоставим разве что только с идентификацией радужки глаза, однако соответствующие устройства ввода этого метода имеют более низкую стоимость. Папиллярный узор пальца человека является уникальной биометрической характеристикой: во всем мире нет двух человек с одинаковым узором. Однако существует одно предубеждение против этого способа, у многих людей появляется ассоциация с преступниками, ведь долгое время это было их "привилегией".

Ни одна из перечисленных выше биометрических технологий распознавания на данный момент не является на 100 % надежной. Не смотря на постоянный технический прогресс, вероятность ошибки или

возможность применения в лучших случаях достигают 90–95 %. Для обеспечения максимальной применимости и уменьшения возможности ошибки применяют комбинации биометрических технологий – многомодальную биометрию.

Существует еще один метод идентификации личности, который дает безошибочные результаты – это идентификация по фрагментам генетического кода. Ни одна из персональных характеристик человека не может сравниться по надежности с генетическим кодом человека. Однако практические способы идентификации, использующие уникальные особенности фрагментов ДНК, в настоящее время применяются редко по причине их сложности и очень высокой стоимости.

Использование на практике всех этих методов идентификации, а точнее их совокупности и приведет к смене документов, удостоверяющих личность. Кардинального изменения могло бы и не потребоваться, достаточно было бы добавить машиносчитываемые поля или штрих-код в документ, но достаточно большое количество информации (об отпечатках пальцев, ДНК...) просто невозможно на них уместить. Альтернативой является пластиковая карточка со встроенным микрочипом. Доступ к информации, записанной на микрочипе удостоверения личности, будет закрыт личным кодом владельца документа. Ее аналог — бесконтактная смарт-карта, обладающая операционной системой, достаточной скоростью передачи и механизмами защиты.

Например, новый загранпаспорт будет представлять собой пластиковую карточку с биометрической информацией (цифровой портрет, цифровой снимок отпечатка пальца с объемом данных 35 Kb), личными сведениями (ФИО, год рождения, место рождения, гражданство и т.д.), служебной информацией и электронным носителем (64Kb). Все эти нововведения предполагают максимальную совместимость с международными стандартами, готовность для перехода к безвизовому режиму с США и Евросоюзом и легкий способ внедрения. Биометрические данные представителя удостоверения будут сканироваться и проверяться с помощью мобильных или стационарных устройств, которыми будут оснащены пропускные пункты. Целостность паспортов является существенным фактором безопасности глобальной транспортной системы, а уверенность органов пограничного контроля в целостности проездных документов государства способствует упрощению формальностей пограничного контроля. Эффективный обмен данными между органами различных стран будет способствовать борьбе с терроризмом и организованной преступностью по всему миру.

Несмотря на то, что биометрия — сравнительно новая область современных информационных технологий, мировой рынок биометрических систем уже сегодня представлен десятками известных фирм. Биометрический рынок развивается быстрыми темпами, уже в 2003 году объем рынка составил более 1 млрд долларов, что опередило самые оптимистические прогнозы.

Коротко об авторах

Жуков А.С., Кутейников К.Ю. – студенты, кафедра «Автоматизированные системы управления», Московский государственный горный университет.

© **В.М. Аленичев, В.И. Суханов,**
2005

УДК 622.271.3.06:004.925.84

В.М. Аленичев, В.И. Суханов