Преимущества системы пропусков занятий, созданной с помощью Microsoft Excel: простота использования; не требует производить самостоятельные расчеты; поиск необходимой информации упрощен за счет гиперссылок; низкая вероятность потери данных (в сравнении с печатными списками); возможность вывести данные на бумажные носители (при необходимости).

Недостаток — большие затраты времени для создания списков.

Заключение. Программа Microsoft Excel за многие годы использования миллионами пользователей по всему миру доказала свою полезность и эффективность, в том числе и для создания системы учета пропусков занятий обучающимися. Данная система будет полезна для контроля пропусков на любом уровне управления в учреждении образования, а также определения суммы для оплаты за них обучающимися.

Список цитируемых источников

1. *Комаровский, А. Н.* Использование условного форматирования в MS Excel для динамического анализа логических схем (рус.) / А. Н. Комаровский // Информатика. — 2007. — № 6. — С. 10—20.

2. *Харвей, Г.* Microsoft Excel 2013 для чайников / Г. Харвей. — М. : Диалектика, 2013. — 368 с.

УДК 004.93

Н. С. Денисенко, Е. Г. Шапович
Учреждение образования «Барановичский государственный университет», Барановичи

БИОМЕТРИЧЕСКАЯ ТЕХНОЛОГИЯ ИДЕНТИФИКАЦИИ НА ОСНОВЕ ОТПЕЧАТКОВ ПАЛЬЦЕВ

Введение. Организация системы контроля и управления доступом — это совокупность программно-аппаратных технических средств, целью которых является регулирование входа людей на заданную территорию или доступа к определенным информационным ресурсам. В свою очередь, управление доступом — это разграничение прав доступа, т. е. определение, кого, в какое время и на какую территорию (к каким ресурсам) допускать.

Идентификация человека по отпечаткам пальцев в настоящее время является лидером среди биометрических технологий. Это достаточно точная, дружественная к пользователю и экономичная технология для применения в области идентификации. Данной технологией в США пользуются, например, ФБР, Секретная служба, Агентство национальной безопасности, министерства финансов и обороны и другие организации. Преимущества доступа по отпечаткам пальцев — простота использования, удобство и надежность. В связи с этим было принято решение разработать систему для идентификации по отпечаткам пальцев.

Основная часть. Актуальность развития биометрических технологий идентификации личности обусловлена увеличением числа объектов и потоков информации, которые необходимо защищать от несанкционированного доступа: криминалистика; системы контроля доступа; системы идентификации личности; системы электронной коммерции; информационная безопасность (доступ в сеть, вход на ПК); учет рабочего времени и регистрация посетителей; системы голосования; проведение электронных платежей; аутентификация на веб-ресурсах; различные социальные проекты, где требуется идентификация людей; проекты гражданской идентификации (пересечение государственных границ, выдача виз на посещение страны) и т. д. [1].

В отличие от бумажных идентификаторов (паспорт, водительские права), пароля или персонального идентификационного номера (PIN), биометрические характеристики не могут быть забыты или потеряны, их трудно подделать и практически невозможно изменить.

Алгоритмы распознавания отпечатков пальцев делятся на два класса: распознавание по отдельным деталям (характерным точкам) и по рельефу всей поверхности пальца [2]. В первом случае устройство анализирует участки, уникальные для конкретного отпечатка, и определяет их взаимное расположение. Во втором случае обрабатывается изображение всего отпечатка. В современных системах часто используется комбинация этих двух способов, что позволяет повысить достоверность идентификации. Регистрация отпечатка пальца человека на оптическом сканере занимает немного времени. Крошечная CCD-камера делает снимок отпечатка пальца. Затем полученное изображение преобразуется в уникальный шаблон отпечатка. Этот шаблон шифруется и записывается в базу данных для аутентификации пользователей. На сегодня использование отпечатка пальца для идентификации личности — самый удобный для пользователя из всех биометрических методов. Качество распознавания отпечатка и возможность его правильной

обработки алгоритмом существенно зависят от состояния поверхности пальца, его положения относительно сканирующего элемента, чистоты пальца и окна сканера, а также от ряда других условий.

Алгоритм сравнения отпечатков по локальным признакам состоит из следующих шагов:

1) улучшение качества исходного изображения отпечатка. Повысить резкость папиллярных линий (хребтов) в найденной маске;

2) бинаризация изображения отпечатка. Преобразовать изображение к черно-белому представлению пороговой обработкой;

3) утончение линий изображения отпечатка. Выполнить утончение бинарного изображения до получения линий шириной 1 пиксел;

4) выделение минуций. Изображение разбить на блоки (например, 9×9 пикселов). Анализируя окрестности каждого пиксела, выделить окончания и раздвоения хребтов;

5) сопоставление минуций. Два отпечатка одного пальца будут отличаться друг от друга поворотом, смещением, изменением масштаба и/или площадью соприкосновения в зависимости от того, как пользователь прикладывает палец к сканеру;

6) принятие решения о совпадении отпечатков. Оценка совпадения отпечатков выполняется по формуле

$$K = \frac{D^2}{pq} 100\ \%,$$

где D — количество совпавших минуций;

p — количество минуций шаблона, хранящегося в базе;

q — количество минуций предъявленного отпечатка.

Если K превышает 65 %, отпечатки считаются идентичными. Для более высокого уровня защиты от незарегистрированного пользователя порог может быть повышен.

Для реализации сервера была выбрана технология ASP.NET Core от компании Microsoft на языке C#.

В приложении используется база данных, содержащая следующие таблицы:

– “Division” — содержит все необходимую информацию о подразделениях предприятия;
– “Fingerprint” — содержит изображение отпечатка и его особые точки;
– “Employee” — содержит всю необходимую информацию о сотрудниках предприятия.

На рисунке 1 представлена физическая модель разработанной базы данных.

На рисунке 2 представлена диаграмма UseCase. Этот вид диаграмм позволяет создать список операций, которые выполняет система. На основе набора таких UseCase-диаграмм создается список требований к системе и определяется множество выполняемых ею функций.

Согласно представленной модели концепция работы приложения заключается в создании информационной базы сотрудников и их идентификации при помощи отпечатка пальца.

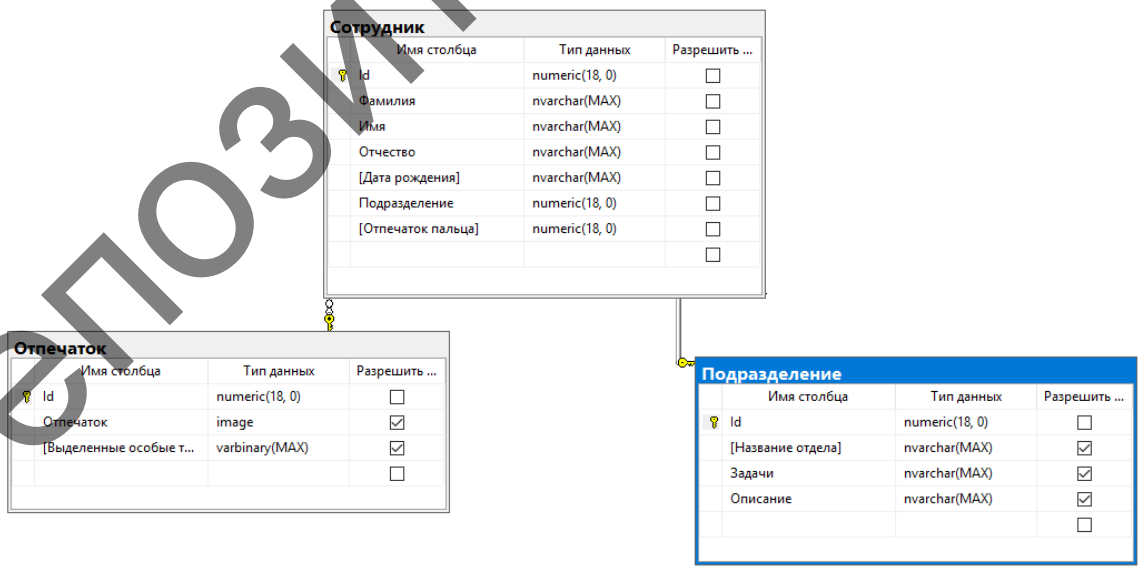

Рисунок 1 — Физическая модель базы данных

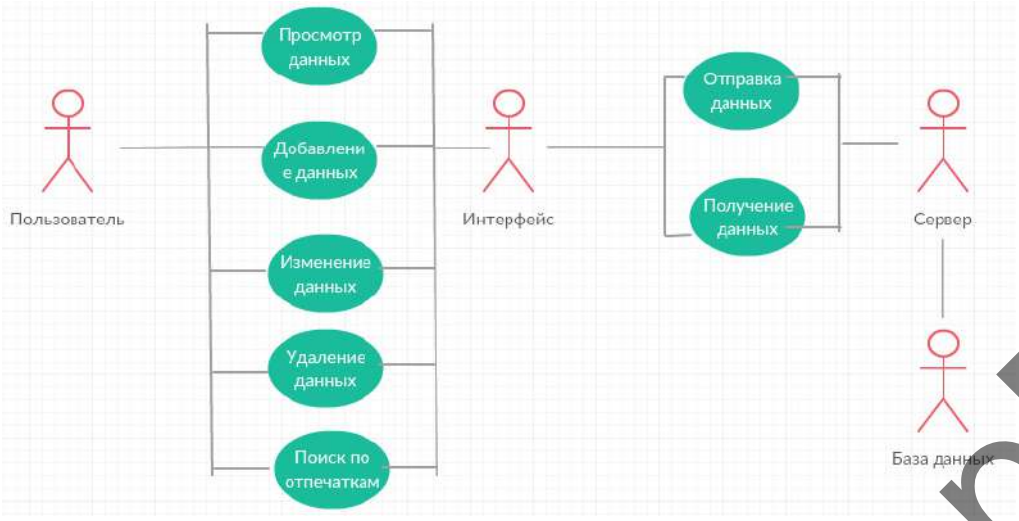

Рисунок 2 — Диаграмма UseCase

Заключение. Сегодня использование отпечатков пальцев при идентификации личности — наиболее простой и комфортный биометрический метод доступа. Поэтому для организации системы контроля и управления доступом людей к определенным информационным ресурсам предлагается использовать биометрическую технологию на основе признаков, извлеченных из отпечатков пальцев.

Список цитируемых источников

1. *Шапович, Е. Г.* Методы распознавания отпечатков пальцев и реализация на высокоуровневом языке программирования C# / Е. Г. Шапович, А. В. Шах // АННИ XXI века: теория и практика. — 2019. — № 1 (44). — С. 477—480.
2. Handbook of fingerprint recognition / D. Maltoni [et al.]. — N. Y. : Springer-Verlag, 2009. — 494 p.

УДК 004.934.2

М. Ю. Ёлкин, А. В. Шах
Учреждение образования «Барановичский государственный университет», Барановичи

РАЗРАБОТКА СИСТЕМЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО ГОЛОСУ

Введение. Биометрическая идентификация личности основана на принципе распознавания и сравнения уникальных характеристик человеческого организма. Уникальность голосовой биометрии состоит в том, что это единственная биометрическая модальность, которая позволяет идентифицировать человека по телефону. Это важно, например, при удаленном доступе к различным услугам, при криминалистической идентификации, где единственным доказательством является запись телефонного разговора подозреваемого. Кроме того, голосовая идентификация не требует применения специализированного дорогостоящего оборудования. Все, что необходимо, — обычный микрофон. При этом по уровню надежности голосовая биометрия не уступает, а по некоторым характеристикам превосходит характеристики других систем биометрической идентификации, таких как почерк, печать на клавиатуре и радужная оболочка глаз.

Уникальность голоса человека обусловлена множеством физиологических особенностей (строением голосовых связок, трахеи, носовых полостей, манерой произношения звуков, расположением зубов). Комбинация этих особенностей индивидуальна, как и отпечатки пальцев. Однако на практике ни одна из унимодальных систем биометрической идентификации, в том числе и голосовая, не может гарантировать 100 %-й идентификации личности. Основными источниками ошибок при идентификации дикторов являются эффекты среды записи (уровень и тип шума, уровень реверберации), представления (длительность речи, психофизиологическое состояние говорящего (болезнь, эмоциональное состояние и т. п.), язык речевого сообщения, изменение голосового усилия), канала (помехи (импульсные, тональные и т. п.), искажения (амплитудно-частотные характеристики микрофона и канала передачи, вид кодирования в канале и т. д.)).

Основная часть. Целью данного проекта является разработка модуля системы биометрической идентификации личности по голосу.