изображения не влияет цвет машин, время суток и небольшие изменения, появляющиеся на изображении (например, прохожие, оказавшиеся в зоне видеонаблюдения). При этом все эти изменения сильно влияют на оценку погрешности *NMSE*.

В связи с этим было принято решение усовершенствовать данную методику, используя оценку уровня резкости изображения, описанную в [3]. Основной задачей являлась установка связи между погрешностью *NMSE* и оценкой уровня резкости изображения. Итоговый алгоритм методики состоит из следующих шагов.

1. Определение порогового и минимального значения *NMSE*.

2. Определение некоторых значений *NMSE* (*NMSE1*, *NMSE2* и т. д.), показывающих, какие фильтры и сколько раз применять.

3. Для всех значений *NMSE* находим соответствующие им оценки уровня резкости изображений ρ (ρmin, ρ1, ρ2 и т. д.) [4].

4. Для следующих подгружаемых изображений определяется только оценка уровня резкости изображения, и в зависимости от того, в какой интервал попадает значение ρ, применяются соответствующие фильтры нужное количество раз.

Разработанная методика нашла широкое применение в соответствующих системах видеомониторинга эксплуатирующихся в режиме реального времени. Она является составляющей частью программного модуля предобработки изображений. Например, время обработки изображения размером 100*30 пикселей на компьютере с процессором Intel Core i5 2.67GHz и ОЗУ 4 Гб составляет 2 мс; время обработки изображения размером 210*50 пикселей на идентичном компьютере составляет 7 мс; время обработки изображения размером 350*100 пикселей составляет 17 мс. Из приведенных временных характеристик совершенно очевидно, что разработанная методика улучшения качества изображений может применяться в системах безопасности, которые непрерывно функционируют в режиме реального времени. Также данная методика активно используется для предобработки изображений при решении задач детекции, распознавания человеческих лиц и номеров транспортных средств [4].

СПИСОК ЛИТЕРАТУРЫ:

1. Цветовая модель RGB. URL: akvis.com.

2. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. М.: Техносфера, 2005. – 1072 с.

3. *Дронов А. Н., Шумилов Ю. Ю.* Комплексная оценка качества изображений для систем видеомониторинга реального времени // Естественные и технические науки. 2009. № 6 (44). С. 485–486.

4. *Дронов А. Н., Шумилов Ю. Ю.* Методы оценки качества изображения // Современные технологии в задачах управления, автоматики и обработки информации: труды XVI Международного научно-технического семинара. Сентябрь 2007 г. Алушта. Тула: Изд-во ТулГУ, 2007. С. 255–256.

А. П. Дураковский, В. Р. Петров

О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В СКУД

В настоящее время *системы контроля и управления доступом* (СКУД) являются неотъемлемым элементом комплексной системы безопасности предприятий и организаций.

Субъект доступа (сотрудник, посетитель) при доступе на объект (охраняемую территорию, помещение) для идентификации должен предъявить какой-либо идентификатор доступа. СКУД на основе установленных администратором политик безопасности и прав субъекта принимает решение о доступе субъекта на объект. При этом в качестве уникальных данных, присущих субъекту доступа, СКУД оперирует сведениями о фамилии, имени, отчестве субъекта, его должности, служебном телефоне, адресе регистрации. В ряде случаев в СКУД фиксируются паспортные данные субъекта и иные сведения [1].

Системы контроля и управления доступом, не учитывающие (не обрабатывающие) **персональные данные** (ПДн), составляют малую часть множества различных СКУД и в настоящее время практически не применяются на предприятиях (примером такой системы является домофон).

Часто встречается мнение, что фамилия, имя, отчество — это не персональные данные. В связи с этим из ИСПДн уплывают не только СКУД (при ведении персонифицированного пропускного режима), но и каталог LDAP (например, AD в случае, если в ней хранятся ФИО пользователей) и т. д.

Для однозначной идентификации лица следует принимать в расчет все средства, в равной мере могущие быть реально использованы либо оператором, либо кем угодно другим для идентификации указанного лица, т. е. к персональным данным относится **любая** информация, об идентифицируемом объекте. По совокупности ряда показателей объект может быть определен конкретно [2].

Продолжим исследования в части биометрических персональных данных. Фотография, видеозапись — это объект ИСПДн или нет? Согласно статье 152.1 ГК РФ, «обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина или его родственников после его смерти. За исключением использования в государственных, общественных или иных публичных интересах или гражданин позировал за плату».

Исходя из определения биометрических ПДн по ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Данные изображения лица», к ним могут быть отнесены фотографии и видеоизображения субъекта ПДн. Фотографии субъекта ПДн могут обрабатываться в:

- пропускных системах;
- системах контроля доступа;
- телефонных и адресных справочниках;
- публикациях и т. д.

Видео субъекта ПДн может обрабатываться в:

- системах видеонаблюдения;
- системах дистанционного обучения и видеообращениях [2].

Какой в общем случае действует алгоритм пропуска?

1-й вариант: посетитель прикладывает пропуск к считывающему устройству, и у охранника высвечиваются его данные. По результатам сличения данных охранник принимает решение о пропуске. В этом случае само по себе фото не является самостоятельно идентифицирующим средством, а идентификация осуществляется по комплексу параметров. Следовательно, изображение гражданина не несет самостоятельной идентифицирующей нагрузки и не может выступать как биометрические ПДн (т. е. данные, которые характеризуют физиологические особенности человека и **на основе которых можно установить его личность**, — см. ч. 1 ст. 11 Закона о персональных данных).

2-й вариант: посетитель прикладывает пропуск к считывающему устройству, и СКУД пропускает посетителя. Охранник контролирует работу СКУД и вмешивается лишь в экстренных

случаях. При этом изображение гражданина вообще практически не используется и необходимо лишь для обеспечения пропуска в случае отключения **СКУД**. И тогда изображение гражданина не несет самостоятельной идентифицирующей информации (т. е. опять не является биометрическими ПДн), а используется в комплексе идентифицирующих факторов.

3-й вариант может быть вообще без фото, но с использованием, например, дактилоскопической или иной биометрической идентификации: посетитель прикладывает к считывающему устройству палец (руку, глаз, др.) и на основании считанной и имеющейся в базе информации СКУД идентифицирует субъекта и пропускает/не пропускает посетителя. В этом случае мы имеем биометрическую систему идентификации.

Таким образом, такие простейшие данные, определяющие личность человека, как ФИО и фотография, — информация для точной идентификации личности, и это наиболее часто используемая информация в каждом организационном субъекте, хранимая в базах данных и наглядно представленная на пропуске на объект. Соответственно, требования приказа ФСТЭК России от 5.02.2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» распространяются и на такие ИСПДн, как СКУД.

СПИСОК ЛИТЕРАТУРЫ:

1. *Ворона В. А., Тихонов В. А.* Системы контроля и управления доступом. М.: Горячая линия — Телеком, 2010. — 272 с.
2. *Лукацкий А. В.* Защита персональных данных и решения Cisco. URL: http://www.orbitacom.ru/images/conf5doc/ 11_Lukatskii.pdf.

Д. В. Калашникова

ТРЕБОВАНИЯ БЕЗОПАСНОСТИ К СИСТЕМАМ ПЛАТЕЖЕЙ НА ОСНОВЕ БЕСКОНТАКТНЫХ КАРТ PAYPASS

Бесконтактные платежи на основе карт MasterCard PayPass — это новая альтернатива безналичного расчета, которая позволяет существенно сократить время, нужное для совершения покупки. Применение такой технологии оплаты полезно в местах, где необходимо быстрое обслуживание клиентов. В основе платежей PayPass лежит радиочастотная технология Near Field Communication ближнего радиуса действия, которая позволяет мгновенно обмениваться данными на расстоянии не более 10 см.

Существенным отличием бесконтактных карт является наличие встроенного бесконтактного чипа, который хранит и обрабатывает данные расчетного счета, а также антенны [1]. Два важных составляющих компонента карты используются для передачи данных по воздуху в считыватель терминала и обратно — от считывателя терминала к карте. Антенна подключается к чипу и, как правило, проходит вблизи периметра карты.

Несмотря на принципиальное отличие в процессе оплаты, для бесконтактной банковской карты наряду с известными угрозами безопасности, характерными для контактных магнитных и микропроцессорных карт, существуют специальные угрозы, связанные с использованием радиоканала для обмена данными. Ниже представлены основные угрозы безопасности бесконтактного радиочастотного интерфейса [2]: