СКУД

Интеграция биометрических контроллеров в ИСО «ОРИОН Про»

Понятие «биометрия» охватывает комплекс различных методов и технологий, позволяющих идентифицировать человека по его биологическим параметрам. Биометрия основана на том, что каждый человек обладает индивидуальным набором физиологических, психосоматических, личностных и прочих характеристик. Например, к физиологическим параметрам можно отнести папиллярные узоры пальцев, рисунок радужной оболочки глаза и т.д.

С возникновением вычислительной техники появились устройства, способные надежно обрабатывать биометрические данные практически в реальном времени, используя при этом специальные алгоритмы. Это послужило толчком в развитии биометрических технологий. В последнее время сферы их применения постоянно расширяются. На рис. 1 представлены некоторые области применения биометрии.

Биометрические параметры

Биометрическая идентификация (БИ) может использовать различные параметры, которые условно можно разделить на 2 типа: статические и динамические (рис. 2).

Статические параметры определяют «материальные» характеристики человека как физического объекта, обладающего определенной формой, весом, объемом и т.д. Эти параметры вообще не меняются или мало меняются в зависимости от возраста человека (это правило может нарушаться только в детском возрасте). Однако не все статические параметры могут использоваться, когда идентификация человека должна проводиться быстро (например, в системах контроля доступа). Очевидно, что анализ ДНК требует довольно существенных временных затрат и вряд ли в ближайшее время будет широко задействован в системах контроля доступа.

Динамические параметры в большей степени описывают поведенческие или психосоматические характеристики человека. Эти параметры могут довольно сильно меняться как в зависимости от возраста, так и при изменяющихся внешних и внутренних факторах (нарушениях здоровья и т.д.). Однако существуют области применения, в которых использование динамических параметров очень актуально, например, при проведении графологических экспертиз или для идентификации человека по голосу.

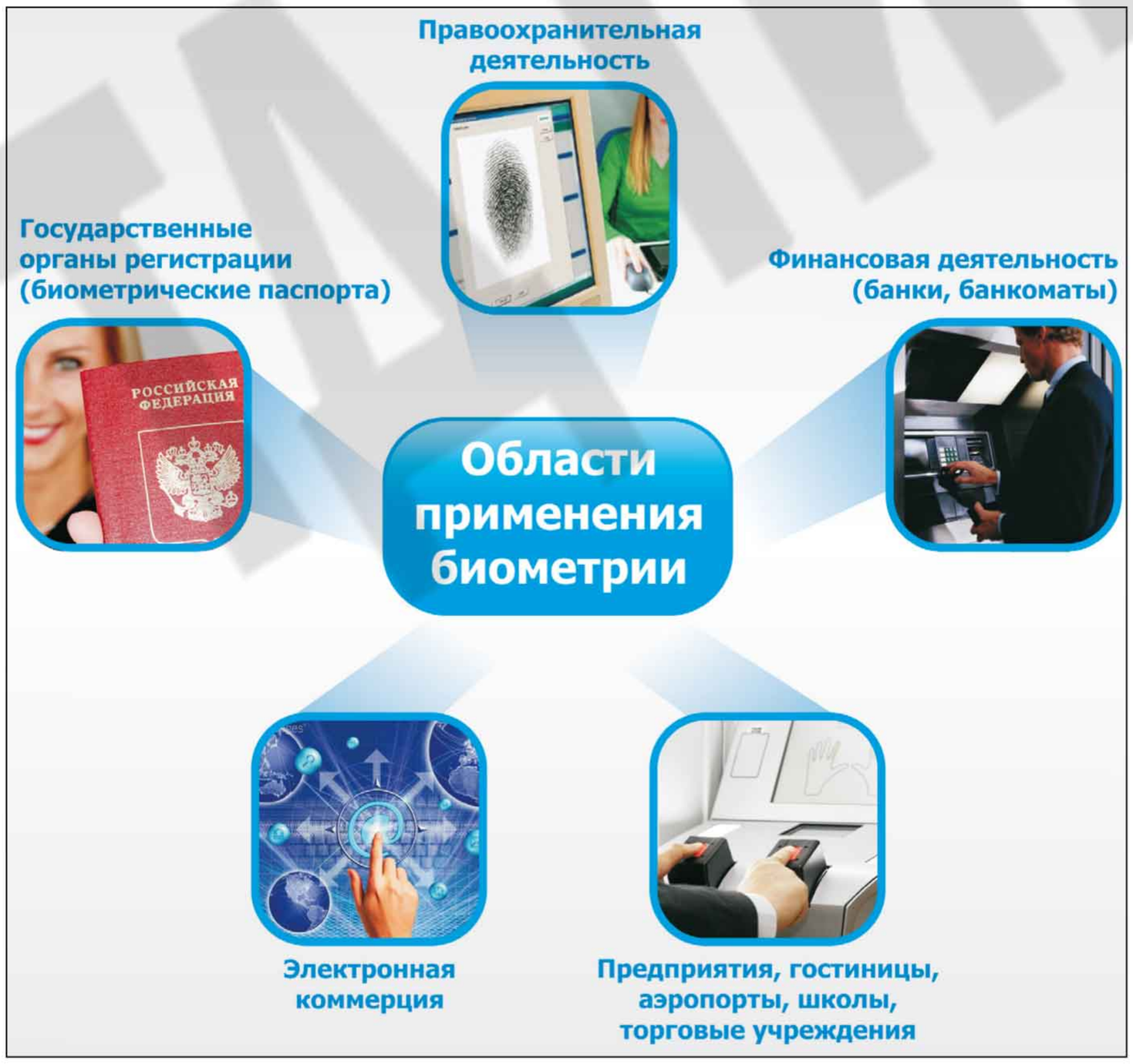

Рис. 1 Области применения биометрии

Достоинства, недостатки и особенности БИ в СКУД

В настоящее время в подавляющем большинстве биометрических систем контроля доступа используются статические параметры. Из них наиболее распространенным параметром являются отпечатки пальцев.

Основными преимуществами использования БИ в СКУД (по сравнению с ключами доступа или проксимити-картами) являются:

- трудности подделки идентификационного параметра;
- невозможность утери идентификатора;
- невозможность передачи идентификатора другому человеку.

Наряду с описанными преимуществами существуют определенные ограничения в применении биометрических систем, связанные с «неточностью» или «размытостью»

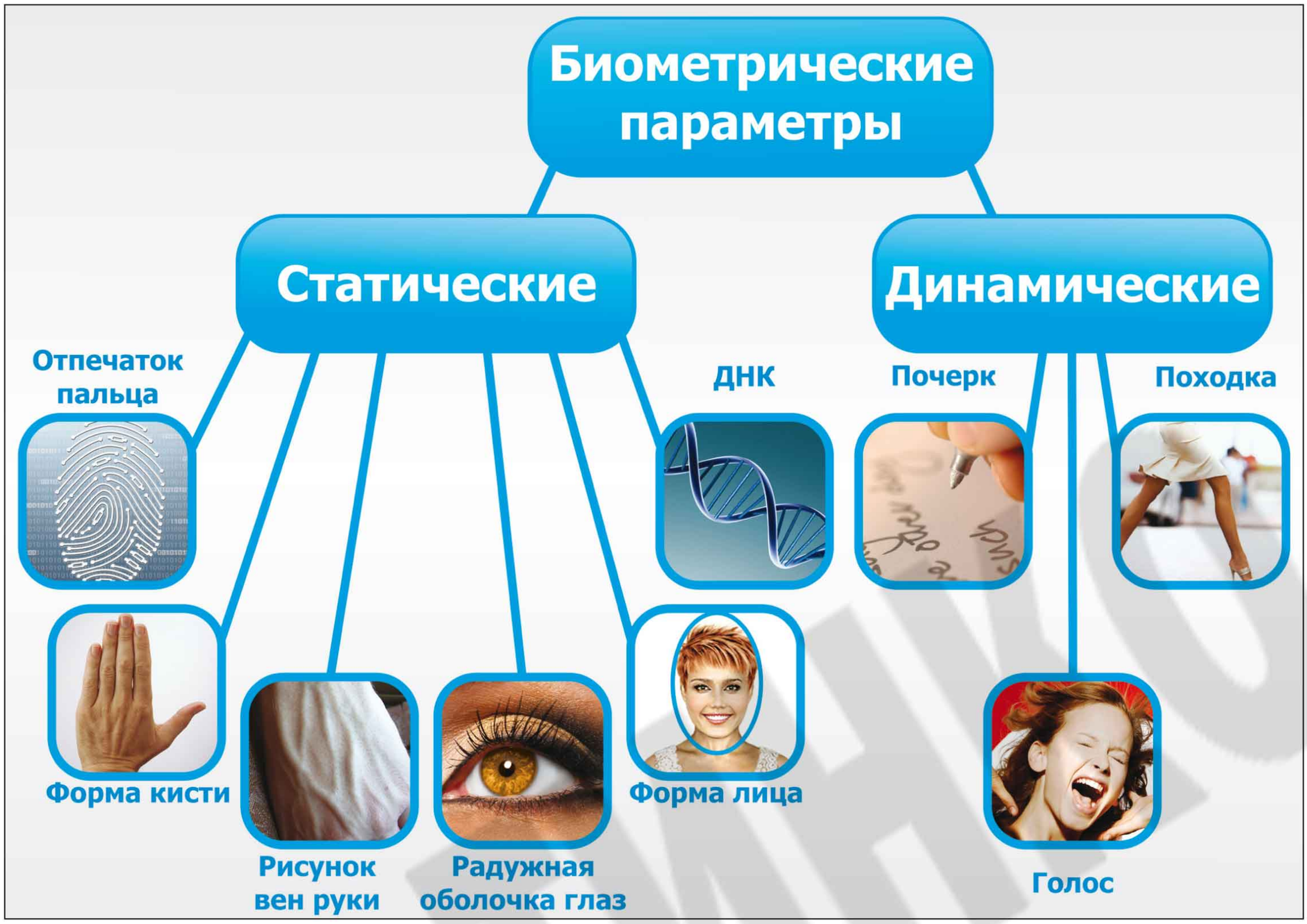

Рис. 2 Типы и виды биометрических параметров

биометрических параметров. Если при использовании проксимити-карты достаточно проверить 2 цифровых кода на полную идентичность, то при сравнении измеренного биометрического параметра с эталонным значением необходимо применять специальные, довольно сложные алгоритмы корреляционного анализа и нечеткой («fuzzy») логики. Это вызвано тем, что при повторном считывании отпечатка пальца или распознавании лица сканер никогда не получит два абсолютно одинаковых изображения. Для решения этой проблемы вместо отсканированных образов используются специальные цифровые модели или шаблоны.

Таким образом, в БИ всегда есть вероятность ошибок двух основных видов:

-ложный отказ в доступе (коэффициент FRR - False Rejection Rate), когда СКУД не распознает (не пропускает) человека, который зарегистрирован в системе,

-ложная идентификация (коэффициент FAR - False Acceptance Rate), когда СКУД «путает» людей, пропуская человека, который не зарегистрирован в системе, то есть распознает его как «своего».

Ситуация осложняется тем, что эти два типа ошибок являются взаимозависимыми. Так, при улучшении параметра FAR, автоматически ухудшится параметр FRR. Другими словами, чем более тщательно система пытается произвести распознавание, чтобы не пропустить «чужого» сотрудника, тем с большей вероятностью она «не узнает своего» (то есть зарегистрированного) сотрудника. Поэтому на практике всегда имеет место некий компромисс между коэффициентами FAR и FRR.

Кроме коэффициентов ошибок идентификации, немаловажным параметром оценки эффективности биометрических систем является скорость идентификации. Это важно, например, на проходных предприятий, когда в короткий промежуток времени через систему проходит большое количество сотрудников. Время срабатывания зависит от многих факторов: метода идентификации, сложности шаблона, количества сотрудников в эталонной базе и т.д. Очевидно, что время срабатывания также коррелирует и с надежностью идентификации – чем более «тщателен» алгоритм идентификации, тем больше система тратит времени на эту процедуру.

Структура биометрической СКУД

Структура биометрической системы доступа включает следующие основные элементы и функции:

- устройство считывания — сканирует биометрический параметр;
- локальная база биометрических параметров — содержит биометрические шаблоны, используемый для идентификации;
- блок идентификации — реали-

Рис. 3 Биометрические контроллеры доступа ИСО «ОРИОН»

зует алгоритм последовательного сравнения считанного шаблона с шаблонами, хранящимися в локальной базе (принцип сравнения «1:N»);

- локальная база стандартных ключей — содержит коды проксимити-карт, PIN-коды, используемые при выборе шаблона для верификации;

- блок верификации — реализует сравнение считанного шаблона с заданным эталонным шаблоном, выбираемым по локальной базе стандартных ключей (сравнение «1:1»);

- информационные интерфейсы RS-485, Ethernet, USB — для информационного обмена;

- сигнальные интерфейсы — обеспечивают прием сигналов от датчиков контактов двери, кнопки «Выход»;

- исполнительные органы — реле, обеспечивающие управление электромеханическими замками и пр.

Описанная структура конструктивно может быть реализована различными способами. При встраивании считывателя отпечатка пальца в панель ноутбука роль остальных элементов выполняет «железо» и программное обеспечение компьютера. Часто на практике применяются распределенные системы с вынесенным биометрическим считывателем, устанавливаемом на границе зоны доступа, в то время как остальные элементы располагаются внутри этой охраняемой зоны. Не менее широко распространены решения, где все элементы биометрической системы выполнены как единый модуль — биометрический контроллер доступа.

Контроллеры C2000-BioAccess-F4 и C2000-BioAccess-F8 в составе ИСО «ОРИОН»

Для развития СКУД на базе ИСО «Орион» в программное обеспечение АРМ «ОРИОН-Про» включена

Рис. 4 Подключение биометрических контроллеров к ИСО «ОРИОН»

поддержка двух биометрических контроллеров – С2000-BioAccess-F4 и С2000-BioAccess-F8 (рис. 3).

Эти контроллеры предназначены для управления доступом с идентификацией по отпечаткам пальцев. Они оснащены оптическим считывателем для сканирования пальца, обеспечивают хранение в локальной базе 2200 шаблонов для идентификации, при этом время идентификации не превышает 1 с. Величины коэффициентов эффективности распознавания FAR и FRR составляют порядка 1% и 0,001% соответственно. Контроллеры могут подключаться к ИСО «ОРИОН» двумя способами: по информационным интерфейсам RS-485 и по Ethernet (рис. 4).

Возможность подключения контроллеров по сети Ethernet позволяет, при наличии «защищенной» локальной сети, без дополнительных затрат на кабельные линии связи организовать СКУД с биометрической идентификацией. Такая система может легко распределяться по зданию или комплексу зданий в соответствии с топологией локальной сети. Вместе с тем, при необходимости, остается возможность «традиционного» подключения биометрических контроллеров по выделенной магистрали RS-485.

Встроенные в контроллеры реле обеспечивают управление электромеханическими замками, кроме этого имеются входы для подключения датчика двери и кнопки «Выход». Наличие в контроллерах клавиатуры и встроенного считывателя смарт-карт позволяет обеспечить работу СКУД в режимах верификации по разным комбинациям параметров доступа, например «карта+палец», «код +палец». В этих режимах контроллер не производит сравнение отпечатка по всей локальной базе шаблонов, а сравнивает считанный отпечаток с единственным шаблоном, который привязан к коду карты доступа или PIN-коду.

Таким образом, контроллеры С2000-BioAccess-F4 и С2000-BioAccess-F8 представляют собой законченные решения для контроля и управления доступом в зоне с одной дверью. Наиболее эффективно данные контроллеры могут использоваться в зонах доступа во внутренние помещения здания с повышенными требованиями по безопасности: банковские хранилища, спецобъекты, помещения повышенной секретности и т.д.

Процедуры и сценарии в ИСО «ОРИОН» с контроллерами С2000-BioAccess-F4 и С2000-BioAccess-F8

Для регистрации нового пользователя в контроллерах предусмотрен специальный режим регистрации отпечатка пальца. При этом для повышения надежности требуется троекратное сканирование пальца, в результате чего контроллер формирует цифровой шаблон. Размер одного шаблона составляет около 500 байт.

Все шаблоны отпечатков пальцев (биометрические ключи), так же, как и обычные ключи, хранятся в центральной базе данных ИСО «ОРИОН». При конфигурировании уровней доступа администратором системы каждый контроллер «привязывается» к определенному уровню доступа, и, таким образом, в его локальную (встроенную) базу шаблонов отпечатков пальцев впоследствии будут записаны шаблоны только тех сотрудников, которые имеют соответствующий уровень доступа.

Если один уровень доступа соответствует нескольким зонам доступа, то возникает необходимость регистрации пользователя во всех контроллерах с таким уровнем доступа. Для решения подобных задач (регистрации, обновления или удаления пользователей) АРМ ИСО «ОРИОН Про» обеспечивает возможность автоматического обмена информацией по всем контроллерам, входящим в конкретный уровень доступа.

Стандартный сценарий администрирования СКУД в ИСО «ОРИОН» с биометрическими контроллерами выглядит следующим образом:

-выделяется отдельный биометрический контроллер для регистрации сотрудников (он может быть установлен, например, в отделе кадров предприятия);

-после успешного прохождения процедуры регистрации шаблон отпечатка пальца (биометрический ключ) зарегистрированного сотрудника автоматически сохраняется в центральной базе данных системы;

-администратор базы данных предоставляет сотруднику (то есть его биометрическому ключу) конкретные права доступа, и система «привязывает» этот ключ к заданным уровням доступа;

-система анализирует уровень доступа биометрического ключа и автоматически «распространяет» этот ключ (цифровой шаблон отпечатка пальца) по всем контроллерам, задействованным в данном уровне доступа, то есть по всем контроллерам, управляющим дверьми, входящими в заданный уровень доступ.

При удалении сотрудника (например, при его увольнении) достаточно удалить из администратора базы данных его биометрический ключ, и система автоматически удалит этот биометрический ключ из всех контроллеров данного уровня доступа.

Такой подход является удобным и достаточно универсальным, что позволяет с успехом использовать его практически во всех организациях.

Таким образом, развитие системы контроля доступа в ИСО «ОРИОН» за счет применения биометрической идентификации на базе контроллеров С2000-BioAccess-F4 и С2000-BioAccess-F8 расширяет функциональные возможности как автономной СКУД, так и интегрированной системы в целом, позволяя реализовать повышенные требования к уровню безопасности или, при необходимости, отказаться от использования ключей доступа и проксимити-карт.

К.Г. Грибачев,
программист ЗАО НВП «Болид»