ИНТЕГРАЦИЯ БИОМЕТРИЧЕСКИХ КОНТРОЛЛЕРОВ В ИСО «ОРИОН»

КОНСТАНТИН ГРИБАЧЕВ

Программист
ЗАО НВП «Болид»
Московская обл.,
г. Королев,
ул. Пионерская, 4.
Тел.: 0 10 7 (495) 775 71 55
e-mail: info@bolid.ru

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 надёжно обрабатывать биометрические данные практически в реальном времени, используя при этом специальные алгоритмы. Это послужило толчком в развитии биометрических технологий.

Достоинства, недостатки и особенности биометрической идентификации в СКУД

В настоящее время наиболее распространённым параметром в подавляющем большинстве биометрических систем контроля доступа являются отпечатки пальцев.

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

- трудности подделки идентификационного параметра;

- невозможность утери идентификатора;

- невозможность передачи идентификатора другому человеку.

Наиболее эффективно перечисленные достоинства используются при организации на основе биометрических систем контроля доступа дополнительного уровня безопасности, т.е. при использовании таких систем совместно с ключами доступа или проксимити-картами.

Наряду с описанными преимуществами существуют определённые ограничения в применении биометрических систем, связанные с «неточностью» или «размытостью» 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 нечёткой (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 биометрической идентификации всегда есть вероятность ошибок двух основных видов:

- ложный отказ в доступе (коэффициент FRR - False Rejection Rate), когда СКУД не распознаёт (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 распознаёт 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 надёжностью 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, которое сканирует биометрический параметр;

- локальную базу биометрических параметров, содержащая биометрические шаблоны, используемые для идентификации;

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

- локальную базу стандартных ключей, содержащую коды проксимити-карт, PIN-коды, используемые при выборе шаблона для верификации;

- блок верификации, который 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, обеспе-

чивающие приём сигналов от датчиков контактов двери и 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 распределённые системы с вынесенным биометрическим считывателем, устанавливаемым 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.

Настольный USB-считыватель отпечатков пальцев С2000-BIOAccess-Z4500K в составе ИСО «ОРИОН»

Данное устройство является считывателем отпечатков пальцев и предназначено для регистрации отпечатков пальцев в центральном компьютере системы. Подключение по интерфейсу USB существенно облегчает процесс подключения считывателя к рабочей станции и повышает эффективность использования. Считыватель оснащен оптическим сенсором с разрешением 500 dpi, а также микроконтроллером, который преобразует изображение отпечатка пальца в специальный формат. Получаемый формат данных полностью совместим с контроллерами С2000-BIOAccess – F4/F8/F18/MA300.

Наличие данного считывателя устраняет необходимость клиентам использовать биометрические контроллеры для процедуры регистрации. Достаточно установить настольный считыватель в отделе кадров, и с помощью Администратора Баз Данных АРМ «Орион ПРО» можно легко и просто регистрировать новых сотрудников. При этом система обеспечит автоматическое прописывание ключей-отпечатков, полученных со считывателя, во все биометрические контроллеры в соответствии с заданными полномочиями доступа.

Контроллер С2000-BIOAccess-F18 в составе ИСО «ОРИОН»

Для развития СКУД на базе ИСО «Орион» в программное обеспечение АРМ «Орион ПРО» была включена поддержка биометрического контроллера С2000-BIOAccess-F18.

Этот контроллер предназначен для управления доступом с идентификацией по отпечаткам пальцев и/или проксимити-картам. Он оснащён оптическим считывателем для сканирования пальца, обеспечивает хранение в локальной базе 2500 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. Контроллер может подключаться к ИСО «ОРИОН» по информационному интерфейсу Ethernet.

Возможность подключения контроллера по сети Ethernet позволяет 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.

Контроллер С2000-BIOAccess-MA300 в составе ИСО «ОРИОН»

Этот контроллер предназначен для управления доступом с идентификацией по отпечаткам пальцев и/или проксимити-картам. Контроллер выполнен в вандалозащищенном исполнении, имеет металлический корпус и класс защиты IP54. Он оснащён оптическим считывателем для сканирования пальца, обеспечивает хранение в локальной базе 1500 шаблонов для идентификации, при этом время идентификации не превышает 1 с.

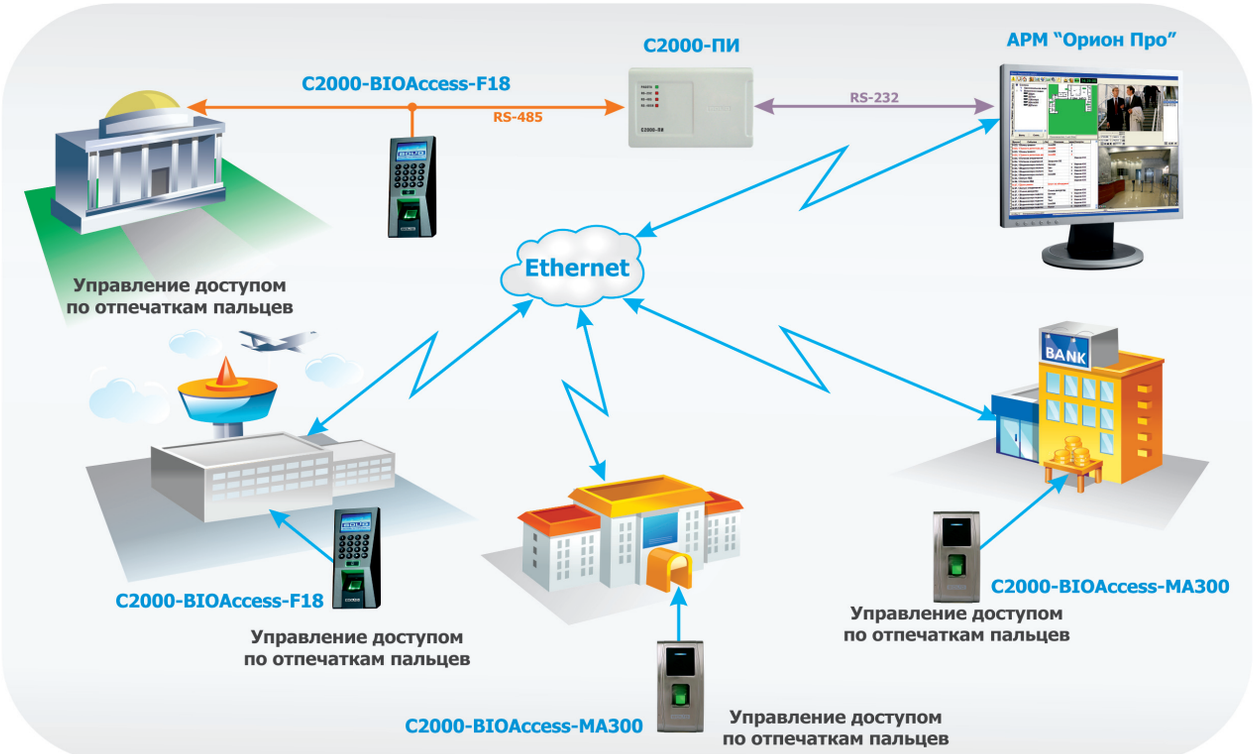
Величины коэффициентов эффективности распознавания FAR и FRR составляют порядка 1% и 0,001% соответственно.

Контроллер может подключаться к ИСО «ОРИОН» по информационному интерфейсу Ethernet. Возможность подключения контроллера по сети Ethernet позволяет, при наличии «защищённой» 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.

Встроенные в контроллер реле обеспечивают управление электромеханическим замком и сиреной, кроме этого имеются входы для подключения датчика двери и кнопки «Выход». Специальное программное обеспечение АРМ «ОРИОН ПРО» позволяет обеспечить работу контроллера и СКУД в режимах верификации по разным комбинациям параметров доступа - «только палец», «только карта», или «карта+палец». В последнем режиме контроллер не производит сравнение отпечатка по всей локальной базе шаблонов, а сравнивает считанный отпечаток с единственным шаблоном, который привязан к коду карты доступа.

Подключение биометрических контроллеров к ИСО «ОРИОН»

Встроенные в контроллеры реле обеспечивают управление электромеханическим замком и сиреной, 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 контроллеры не производят сравнение отпечатка по всей локальной базе шаблонов, а сравнивают считанный отпечаток с единственным шаблоном, который привязан к коду карты доступа или PIN-коду.

Таким образом, контроллеры С2000-BIOAccess-F18 и С2000-BIOAccess-MA300 представляют собой законченное решение для контроля и управления доступом в зоне с одной дверью. Наиболее эффективно они могут использоваться в зонах доступа зданий с повышенными требованиями по безопасности: банковские хранилища, спецобъекты, помещения повышенной секретности и т.д.

Процедуры и сценарии в ИСО «ОРИОН» с С2000-BIOAccess-F18 и С2000-BIOAccess-MA300

Для регистрации нового пользователя в контроллере предусмотрен специальный режим регистрации отпечатка пальца. При этом для повышения надежности требуется трёхкратное сканирование пальца, в результате чего контроллер формирует цифровой шаблон. Размер одного шаблона составляет около 600 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 определённому 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 «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 записывает этот ключ (цифровой шаблон отпечатка пальца) во все контроллеры, управляющие дверями, входящими в заданный уровень доступа.

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 счёт применения биометрической идентификации на базе контроллеров С2000-BIOAccess-F18 и С2000-BIOAccess-MA300 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.