УДК 004.4
DOI: 10.18101/978-5-9793-1397-9-70-74

ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКИХ ДАННЫХ

© **Макшанова Лариса Михайловна**
кандидат технических наук, доцент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
E-mail: lorimak@list.ru

© **Васюкова Олеся Петровна**
студент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
E-mail: olesya.vasyukova@mail.ru

В статье рассмотрена система контроля учета доступа (СКУД) для приборостроительного завода. Тема статьи является актуальной для каждой современной организации, в которой действует контрольно-пропускной режим, будь то промышленное предприятие или вуз. Даже современные гаджеты оборудованы идентификационными биометрическими сканерами.

На приборостроительном заводе действует система СКУД, использующая карты доступа и метки, однако происходит идентификация самой метки, а не человека. Карту доступа можно легко потерять, передать третьему лицу. С биометрией такие случаи полностью исключены

Ключевые слова: биометрия; идентификационные биометрические сканеры; идентификация.

Введение

Проблема создания быстрого и надежного способа аутентификации человека была и остается одной из самых актуальных. Традиционные процедуры проверки соответствия осуществляются с помощью информации, которую знает человек (пароль), и / или физических компонентов (например, идентификационные брелоков или смарт-карт).

Идентификация человека по его биометрическим параметрам имеет очевидное преимущество по сравнению с традиционным методами.

Что такое биометрические данные и зачем их собирают?

Биометрические данные — это уникальные биологические и физиологические характеристики, которые позволяют установить личность человека [2].

Существует пять наиболее распространенных типов биометрии: отпечаток пальца, изображение лица, голос, радужная оболочка глаза и рисунок вен ладони и пальца. Биометрию используют в цифровой идентификации граждан.

Биометрия — это уникальный «ключ», который нельзя потерять и практически невозможно подделать.

Как начать пользоваться биометрическими данными и насколько это надежно?

Нужно зарегистрироваться в Единой биометрической системе. Для этого вам нужно стать клиентом банка, например, открыть счет. Сотрудник банка поможет завести учетную запись на «Госуслугах» (если у вас ее нет), соберет ваши биометрические данные — сфотографирует и запишет голос, а затем отправит эти данные в Единую биометрическую систему. После этого вы сможете дистанционно получать услуги банков, предоставляемые по удаленной идентификации. Нужно будет ввести логин и пароль «Госуслуг», а затем произнести контрольную фразу, глядя в камеру смартфона или компьютера: система вас распознает и доступ к услугам откроется [1].

Допустим, если биометрией будут пользоваться близнецы, тогда точность распознавания их биометрических алгоритмов будет намного выше, чем стандартная аутентификация. Например, если один из близнецов придет в банк и попробует открыть счет на имя другого, то вполне возможно, что у него это получится и операционист не заметит подвоха. С биометрической системой такое не сработает: во-первых, применяется двухфакторная идентификация — алгоритмы распознают людей не только по лицу, но и по голосу (а даже у близнецов он разный), во-вторых, для идентификации в системе нужно знать логин и пароль от «Госуслуг» — это гарантирует дополнительную защиту данных.

1. Анализ биометрии в мировой практике и в России

Крупнейшая в мире база биометрических данных существует в Индии. В системе Aadhaar зарегистрировано более 80% населения страны, биометрия используется в разных сферах — финансах, туризме, образовании и государственных услугах.

В России биометрические технологии только развиваются: пока процедуру биометрической идентификации запустило только девять банков. Со временем Единую биометрическую систему начнут использовать в медицине, образовании, ритейле и других отраслях [1].

Выбор технологии

Существуют следующие биометрические технологии распознавания личности:

- идентификация по отпечаткам пальцев (можно подделать слепок руки, у пожилых людей чаще срабатывают отказы, затруднена идентификация из-за грязных и влажных рук);
- идентификация по радужной оболочке (долгое идентифицирование, неудобное использование);
- распознание по лицу (система пропускает даже фотографию, лицо может измениться с возрастом);
- распознание по сетчатке глаза (сложно и дорого использовать);

- распознание по венам руки (высокая достоверность, отсутствие контакта со считывателем, быстрый ответ системы, реакция только на живую руку, не считывается внешнее состояние руки);
- геометрия рук (метод не получил широкого применения).

Следует отметить, что технологии идентификации постоянно совершенствуются, возможно, в скором будущем появятся и другие биометрические методы. Сегодня метод идентификации по уникальному рисунку вен ладоней признан самым надежным и удобным в использовании.

Инфракрасная камера делает снимки внешней или внутренней сторон руки. Рисунок вен формируется благодаря тому, что гемоглобин крови поглощает ИК-излучение. Вены видны на камере в виде черных линий, а специальная программа на основе полученных данных создает цифровую свертку [1].

На приборостроительном заводе очень много работающих пенсионеров, поэтому устройства должны быть максимально простыми, быстрыми, не доставляющими дискомфорт работникам. В данной статье более подробно рассмотрим технологию идентификации личности по рисунку вен на ладони, скорость ответа которой велючает:

- время регистрации (2 изображения + верификация) — 5–8 с;
- время верификации около 0,8 с (сравнение образа руки на карте и образа руки работника);
- время идентификации около 1–2 с (сравнение образа руки работника со всеми образами в базе данных).

В часы пик на проходной завода должно быть идентифицировано до 1000 работников за 30 минут (рис. 1).

Для данного способа идентификации используется следующее активное оборудование:

- считыватель PalmSecure Sensor (для идентификации);
- сканер PalmSecure v.2 (для записи образа вен ладони);
- устройство крэдл для встраивания в стену или турникет;
- терминал учета рабочего времени (полностью автоматизирует табельную систему, синхронизирован с 1С);
- контроллер для управления турникетами, дверьми, замками [1].

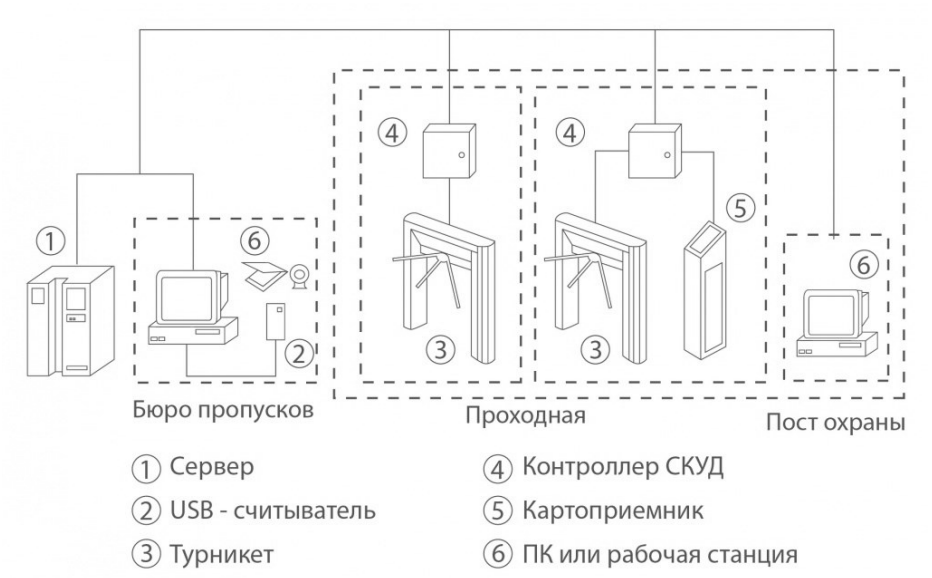

Рис. 1. Схема готового решения

Проектируемая сеть позволит:

- при высоких начальных вложениях обеспечить существенную экономию полных затрат;
- полностью автоматизировать учет рабочего времени;
- усовершенствовать действующую систему контроля доступа;
- создать центральный биометрический архив [2].

Заключение

Данная статья может служить обоснованием для внедрения новой технологии в дополнение к существующей системе управления контролем доступа на Улан-Удэнском приборостроительном заводе, что полностью исключит вероятность несанкционированного проникновения на его территорию.

Литература

1. Афанасьев А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учеб. пособие для вузов. М., 2012. 254 с.

2. Яковлев В. Б. Биометрическая обработка экспериментальных данных: монография. М. : Нобель Пресс, 2014. 376 с.

INFORMATION PROTECTION USING BIOMETRIC DATA

Larisa M. Makshanova
Cand. Sci. (Engineering), Senior Lecturer,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: lorimak@list.ru

Olesya P. Vasyukova
Student,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: olesya.vasyukova@mail.ru

This topic of the article is relevant for every modern organization where the access control regime is in effect, be it an industrial enterprise or a university. Even modern gadgets are equipped with identification biometric scanners.

The Instrument-Making Plant operates an ACS system using access cards and tags, however, the tag itself is identified, not the person. Access card can be easily lost, transferred to a third party. With biometrics, such cases are completely excluded.

Keywords: biometrics; identification biometric scanners; identification.