Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 9, Is. 3, pp. 129-134, 2016

DOI: 10.13187/vesp.2016.9.129
www.ejournal21.com

UDC 004.056.53

Application of Biometric Methods in Control System and Access Control

Natalya S. Ralnikova[a, *], Xenia A. Kudryavtseva [a]

[a] ITMO University, Russian Federation

Abstract

Advantages of biometric identifiers based on unique biological, physiological characteristics of the person uniquely identity has led to intense development of appropriate tools. This article analyzes the biometric methods used in monitoring systems and access control, special attention is paid to the advantages and disadvantages of each method. In the conclusion the authors come to the conclusion that it is impossible to single out the best or the worst methods, as each of them can be used depending on the task. Also, as a conclusion is an example of the use of biometric methods in the control system and access control.

Keywords: control systems and access control, biometrics, biometric identification, identification by the iris of the eye, fingerprint identification.

1. Введение

Информационная безопасность любого предприятия основывается на системах контроля и разграничения доступа. Необходимость в них объясняется тем, что требуется контроль нахождения посторонних, несанкционированных лиц в контролируемой зоне объекта. При работе с информационной базой пользователи должны иметь возможность получить необходимую им информацию – справочники товаров и продукции, документы клиентов, цены и т.д. Однако каждый пользователь должен иметь доступ только к той информации, которая ему требуется для выполнения своих обязанностей, и не иметь доступа к информации, ответственным за которую он не является.

Используются как устаревшие методы визуализации (предъявление вахтеру соответствующих документов), так и автоматической идентификации входящих/выходящих работников и посетителей. Различные автоматические системы контролируемого обеспечения доступа можно разделить на три группы в соответствии с тем, что человек собирается предъявлять системе: секретные данные (пароль, PIN), персональный идентификатор (пластиковая карта, токен, также широко используются малогабаритные пульты-ключи типа Touch Memory.), либо свои персональные характеристики – биометрические данные (Каторин, 2015).

* Corresponding author
E-mail addresses: natalya.ralnikova@gmail.com (N.S. Ralnikova), kudriavtseva.ksyu@yandex.ru (X.A. Kudryavtseva)

2. Материалы и методы

Основным источником для написания данной статьи стали последние исследования в области систем контроля доступа и организационных методов регулирования нахождения персонала в контролируемой зоне, которые показывают, что треть пользователей записывает пароли, а это означает, что любые носители информации о пароле (как правило, это обычный листок бумаги, оставленный в ящике стола) могут быть доступны другим лицам.

Методологическую основу данного исследования составили логические приемы, определения, описания, анализа и синтеза. Также использован общенаучный метод анализа.

3. Обсуждение

Понятие «биометрия» определяет раздел биологии, занимающийся количественными биологическими экспериментами с привлечением методов математической статистики. Биометрия представляет совокупность автоматизированных методов и средств идентификации человека, основанных на его физиологических или поведенческих характеристиках. В отличие от паролей и носителей информации, которые могут быть потеряны, украдены, скопированы, биометрические системы доступа основаны на человеческих параметрах, которые всегда находятся вместе с ними, и проблема их сохранности не возникает (Черкезов, 2006; Мальцев, 2011).

Использование биометрической идентификации в службе информационной безопасности предприятия, в первую очередь, позволит ограничить доступ к компьютерам (рабочим станциям и серверам), к базам данных либо их частям, обеспечит контроль личности оператора в реальном режиме времени.

На данный момент существует достаточно много способов биометрической аутентификации. Все они делятся качественно на две большие группы, а именно: статические и динамические методы биометрической аутентификации. Уникальные физиологические, или по-другому статические, характеристики каждого человеческого организма, которые он получает от бога и природы и присущие только ему - составляют основу статических методов биометрической аутентификации. Статические характеристики человека не меняются на протяжении всей его жизни и являются неотъемлемыми от него.

Все биометрические системы работают практически по одинаковой схеме. Принцип работы таких систем основан на получении изображения со сканера биометрического считывателя и его преобразовании в некий шаблон, который затем сравнивается с имеющейся базой (Попов, 2002; ГОСТ Р 51241-2008).

В момент сравнения полученного изображения с шаблоном возможно появление ошибок: ошибки первого рода – когда сканер не может распознать зарегистрированного пользователя и ошибки второго рода – когда незарегистрированный пользователь определяется системой как зарегистрированный (Каторин, 2015).

Динамические методы биометрической аутентификации основываются на поведенческой (динамической) характеристике человека, то есть, построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия (Fisher, 1997).

1) По рукописному почерку. Метод биометрической аутентификации по рукописному почерку основывается на специфическом движении человеческой руки во время подписания документов. Сложность метода заключается в том, что при каждом подписывании автором могут добавляться некоторые фрагменты подписи, так же как некоторые фрагменты могут сливаться там, где в образце этого нет. Также серьезной проблемой является сильная зависимость параметров системы от психологического состояния людей и стабильности их почерка.

2) По клавиатурному почерку. Возможность аутентифицировать клавиатурный почерк человека появляется при вводе в качестве пароля фразы, состоящей из достаточно большого количества букв. Индивидуальность пользователя полагается в скорости набора символов, разных привычек по поводу нажатий клавиш и т. д. Достоинством данного метода является то, что для идентификации личности не требуется никакого дополнительного оборудования кроме стандартной клавиатуры.

3) По голосу. Данному методу не требуется дорогостоящая аппаратура, достаточно микрофона и звуковой платы. Система анализирует несколько произношений контрольной фразы, на основе чего создается биометрический эталон, который, по сути, предсказывает наиболее вероятные значения характерных функций. Недостатком системы служит невозможность сохранения контрольной фразы в тайне. Поэтому современные ожидания эффективности систем аутентификации по голосу базируются на предположении о возможности такой аутентификации при произнесении произвольной фразы (Каторин, 2013, 2015; Fisher, 1997).

Статические методы биометрической аутентификации основаны на физиологических характеристиках человека, присутствующих от рождения и до смерти, находящиеся при нём в течение всей его жизни, и которые не могут быть потеряны, украдены и скопированы (Егупов, 2004).

1) Отпечатки пальцев. Идентификация по отпечаткам пальцев – это наиболее распространенный биометрический метод идентификации личности. Метод использует уникальность рисунка папиллярных узоров на пальцах людей. Отпечаток, полученный с помощью сканера, преобразовывается в цифровой код, а затем сравнивается с ранее введенными наборами эталонов. Преимущества использования аутентификации по отпечаткам пальцев - легкость в использовании, быстрота и удобство, а также сравнительно маленькая стоимость оборудования. К недостаткам же данного метода относятся невозможность идентификации при царапинах, порезах и ожогах пальцев, а также недостаточная защищенность от подделки, что связано с широким распространением данного метода.

2) Радужная оболочка глаза. Это тонкая подвижная диафрагма глаза у позвоночных с отверстием (зрачком) в центре. Радужная оболочка по текстуре напоминает сеть с большим количеством окружающих кругов и рисунков, которые могут быть измерены компьютером. Программа сканирования радужной оболочки глаза использует около 260 точек привязки для создания образца. Поэтому данный метод является наиболее точным (Мальцев, 2011). К недостаткам данного метода можно отнести высокую стоимость оборудования, а к достоинствам – высокую точность метода и отсутствие физического контакта со сканером.

3) Сетчатка глаза. Метод идентификации по сетчатке глаза основывается на уникальности рисунка кровеносных сосудов глазного дна. Сканирование сетчатки происходит с использованием инфракрасного света низкой интенсивности, направленного через зрачок к кровеносным сосудам на задней стенке глаза. Из полученного сигнала выделяется несколько сотен особых точек, информация о которых сохраняется в шаблоне (Мальцев, 2011). Подобные системы требуют чёткого изображения и, как правило, чувствительны к неправильной ориентации сетчатки. Поэтому требуется смотреть очень аккуратно, а наличие некоторых заболеваний может препятствовать использованию данного метода. Также к недостаткам относится высокое время обработки. К достоинствам можно отнести очень низкую вероятность ошибок.

4) Геометрия лица. Существует множество методов распознавания по геометрии лица. Все они основаны на том, что черты лица и форма черепа каждого человека индивидуальны (Черкезов, 2006; Каторин и др., 2012). К недостаткам данного метода можно отнести то, что многие алгоритмы не учитывают возможные изменения мимики лица, то есть выражение должно быть нейтральным. Преимуществом является возможность распознавания на значительных расстояниях от камеры.

5) Термограмма лица. Исследования показали, что распределение на лице кровеносных сосудов уникально, поэтому его можно использовать для биометрической идентификации. Для получения термограммы лица, которая затем преобразуется в шаблон, используется инфракрасная камера, которая улавливает количество тепла, выделяемого сосудами лица. Достоинство в том, что использование специальных масок, проведение пластических операций, старение организма человека, температура тела, охлаждение кожи лица в морозную погоду не влияют на точность термограммы. Недостатком является невысокое качество аутентификации (Каторин и др., 2013).

6) Карта вен. Данный метод идентификации является наиболее новым. Инфракрасная камера делает снимки внешней или внутренней стороны руки. Результаты такого сканирования не зависят от загрязнений или повреждений поверхностных кожных

покровов, к тому же, этот способ довольно быстр. Рисунок вен формируется благодаря тому, что гемоглобин крови поглощает ИК излучение. В результате, степень отражения уменьшается, и вены видны на камере в виде черных линий. Специальная программа на основе полученных данных создает цифровую свертку (Мальцев, 2011).

Считается, что пространственная структура вен уникальна даже у однояйцовых близнецов и не меняется на протяжении всей жизни, а лишь пропорционально увеличивается, являясь, таким образом, биометрическим идентификатором личности человека. Достоинство – не требуется контакта человека со сканирующим устройством. Вместе с тем, многие возрастные заболевания могут затруднить идентификацию, привести к ошибке второго рода – это явный недостаток данного метода (Каторин, 2015).

4. Результаты

Из анализа представленных выше методов можно сделать вывод о том, что каждый из них имеет как преимущества, так и недостатки, и могут применяться в зависимости от поставленной задачи. Например, самый быстрый метод – метод сканирования отпечатков пальцев, однако он не достаточно надежный, и если необходима более надежная система, то следует использовать метод распознавания по радужной оболочке, однако этот метод будет более дорогостоящим. Для массового распознавания людей лучше всего подходят методы идентификации по геометрии лица (Fisher, 1997).

В качестве примера можно рассмотреть систему для контроля физического доступа сотрудников на предприятие. Для этого вполне подойдет система, использующая метод идентификации по отпечатку пальца. Проходная объекта может быть оборудована следующей системой:

- BioSmart 5M-O-EM – Контроллер BioSmart 5M-O предназначен для идентификации пользователей по отпечаткам пальцев и RFID картам. Позволяет управлять замком, турникетом (в одну сторону), другими исполнительными устройствами. Интерфейсы Ethernet и USB для связи с компьютером, WEB интерфейс для конфигурирования параметров.

- Турникет-трипод PERCo-TTR-04.1G. Высокая пропускная способность позволяет применять турникеты в условиях большого потока людей. Специальное демпфирующее устройство обеспечивает плавный поворот планок до исходного состояния после каждого прохода. Встроенные датчики поворота планок позволяют фиксировать реальный факт прохода, что обеспечивает корректную работу турникета.

5. Заключение

Недостатки методов парольной аутентификации, а также методов с использованием физических идентификаторов, привели к осознанию необходимости использования биометрических систем контроля и управления доступом. В данной статье был проведен анализ методов биометрических систем контроля и управления доступом, выявлены преимущества и недостатки различных методов, а также представлено решение оборудования проходной предприятия с использованием биометрической системы для контроля физического доступа.

Преимущество биологических систем идентификации, по сравнению с традиционными (например, PIN-кодовыми, доступом по паролю), заключается в идентификации не внешних предметов, принадлежащих человеку, а самого человека. Анализируемые характеристики человека невозможно утерять, передать, забыть и крайне сложно подделать. Они практически не подвержены износу и не требуют замены или восстановления.

Примечания

Каторин, 2015 - *Каторин Ю.Ф.* Методы и средства биометрической идентификации личности // Вестник полиции, 2015. Vol.(4), Is. 2.

Каторин, Ныpков, Соколов, Ежгуров, 2013 - *Каторин Ю.Ф., Ныpков А.П., Соколов С.С., Ежгуров В.Н.* Основные принципы построения защищенных информационных систем автоматизированного управления транспортно-логическим комплексом. // *Проблемы информационной безопасности. Компьютерные системы,* 2013. № 2, с. 54-58.

Черкезов, 2006 - *Черкезов Р.* (2006). Динамические методы биометрической аутентификации личности (2006). URL:http://re.mipt.ru/infsec/2006/essay/2006_Dynamic_biometric_authentification__Cherkezov.pdf

Мальцев, 2011 - *Мальцев А.* (2011). Современные биометрические методы идентификации (2011). URL: http://habrahabr.ru/post/126144/.

Попов, 2002 - *Попов М.* (2002). Биометрические системы безопасности // БДИ №1(41). URL: http://www.bre.ru/security/12571.html.

ГОСТ Р 51241-2008 - *ГОСТ Р 51241-2008.* Средства и системы контроля и управления доступом. Классификация.

Каторин, 2013 - *Каторин Ю.Ф.* Проблемы аутентификации с использованием биометрических характеристик. Материалы научной конференции по проблемам информатики. СПб.: НИУ ИТМО, 2013. с. 688–691.

Егупов, 2004 - *Егупов Н.Д.,* Пупков К.А. Методы классической и современной теории автоматического управления. Том 2. Статистическая динамика и идентификация систем автоматического управления. М.: МГТУ им. Н.Э. Баумана, 2004.

Каторин, Коротков, Ныркov, 2012 - *Каторин Ю.Ф. Коротков В.В., Ныркov А.П.* Защищенность информации в каналах передачи данных в береговых сетях автоматизированной идентификационной системы. // Журнал университета водных коммуникаций, 2012. №1 (13), с. 98-102.

Fisher, 1997 - *Fisher R.A.* (1997). On an Absolute Criterion for Fitting Frequency Curves. Statistical Science, vol.12, No. 1, pp. 39-41.

References

Katorin, 2015 - *Katorin Yu.F.* (2015). Metody i sredstva biometricheskoi identifikatsii lichnosti // Vestnik policii, Vol.(4), Is. 2.

Katorin, Nyrkov, Sokolov, Ezhgurov, 2013 - *Katorin Yu.F., Nyrkov A.P., Sokolov S.S., Ezhgurov V.N.* (2013). Osnovnye printsipy postroeniya zashchishchennykh informatsionnykh sistem avtomatizirovannogo upravleniya transportno-logicheskim kompleksom. SPb.: Problemy informatsionnoi bezopasnosti. Komp'yuternye sistemy, № 2, s. 54-58.

Cherkezov, 2006 - *Cherkezov R.* (2006). Dinamicheskie metody biometricheskoi autentifikatsii lichnosti (2006). URL: http://re.mipt.ru/infsec/2006/essay/ 2006_Dynamic_ biometric_authentification__Cherkezov.pdf

Mal'tsev, 2011 - *Mal'tsev A.* (2011). Sovremennye biometricheskie metody identifikatsii (2011). URL: http://habrahabr.ru/post/126144/.

Popov, 2002 - *Popov M.* (2002). Biometricheskie sistemy bezopasnosti // BDI №1(41). URL: http://www.bre.ru/security/12571.html.

GOST R 51241-2008 - GOST R 51241-2008. Sredstva i sistemy kontrolya i upravleniya dostupom. Klassifikatsiya.

Katorin, 2013 - *Katorin Yu.F.* (2013). Problemy autentifikatsii s ispol'zovaniem biometricheskikh kharakteristik. Materialy nauchnoi konferentsii po problemam informatiki. SPb.: NIU ITMO, s. 688–691.

Egupov, 2004 - *Egupov N.D.* (2004). Pupkov K.A. Metody klassicheskoi i sovremennoi teorii avtomaticheskogo upravleniya. Tom 2. Statisticheskaya dinamika i identifikatsiya sistem avtomaticheskogo upravleniya. M.: MGTU im. N.E. Baumana.

Katorin, Korotkov, Nyrkov, 2012 - *Katorin Yu.F. Korotkov V.V., Nyrkov A.P.* (2012). Zashchishchennost' informatsii v kanalakh peredachi dannykh v beregovykh setyakh avtomatizirovannoi identifikatsionnoi sistemy. SPb.: Zhurnal universiteta vodnykh kommunikatsii, №1 (13), s. 98-102.

Fisher, 1997 - *Fisher R.A.* (1997). On an Absolute Criterion for Fitting Frequency Curves. *Statistical Science*, vol.12, No. 1, pp. 39-41.

УДК 004.056.53

Применение биометрических методов в системах контроля и управления доступом

Н.С. Ральникова [a], К.А. Кудрявцева [a]

[a] Университет ИТМО, Российская Федерация

Аннотация. Достоинства биометрических идентификаторов на основе уникальных биологических, физиологических особенностей человека, однозначно удостоверяющих личность, привели к интенсивному развитию соответствующих средств. В данной статье проводится анализ биометрических методов, применяемых в системах контроля и управления доступом, особое внимание уделяется достоинствам и недостаткам каждого из методов. В заключении авторы приходят к выводу, что нельзя выделить лучшие или худшие методы, так как каждый из них может применяться в зависимости от поставленной задачи. Также, в качестве заключения приводится пример применения биометрических методов в системе контроля и разграничении доступа.

Ключевые слова: системы контроля и управления доступом, биометрия, биометрическая идентификация, идентификация по радужной оболочке глаза, идентификация по отпечаткам пальцев.