DOI: 10.58168/ROBOTICS2024_77-86
УДК 004.78:681.139.3

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКИХ ХАРАКТЕРИСТИК ЛИЧНОСТИ

CONTROL AND ACCESS MANAGEMENT SYSTEM USING BIOMETRIC PERSONAL CHARACTERISTICS

Плотников А.О., студент
Стариков А.В., д.т.н., доц.
ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»
г. Воронеж, Россия
star123@yandex.ru

Plotnikov A.O., student
Starikov A.V., DSc (Engineering), Associate Professor
FSBEI HE "Voronezh State University of Forestry and Technologies named after G.F. Morozov"
Voronezh, Russian Federation

Аннотация: В статье рассмотрены основные понятия и возможности системы контроля и управления доступом, особенности автоматизации процесса идентификации личности с использованием биометрических характеристик.

Abstract: The article discusses the basic concepts and capabilities of the access control and management system, the features of automating the process of personal identification using biometric characteristics.

Ключевые слова: контроль и управление доступом, система контроля и управления доступом (СКУД), биометрические характеристики личности, автоматизация.

Keywords: control and access management, access control and management system (ACMS), biometric personal characteristics, automation.

Система контроля и управления доступом (СКУД) представляет собой совокупность программно-технических и организационно-методических

средств, с помощью которых осуществляется контроль и управление доступом на охраняемый объект (предприятие, организацию и др.), а также оперативный контроль за передвижением персонала и временем его нахождения на объекте.

СКУД предназначена для обеспеченияустановленного контрольно-пропускного режима и ограничивает (предотвращает) несанкционированный доступ лиц, не имеющих соответствующих прав, на контролируемый объект или к определенной аппаратуре, техническим средствам и предметам. СКУД также может осуществлять контроль перемещения людей и транспорта по территории объекта, обеспечивать безопасность персонала и посетителей, а также способствовать сохранности материальных и информационных ресурсов [1].

Установление подлинности и определение полномочий субъекта при его допуске на охраняемый объект выполняется в ходе идентификации субъекта. Процедура идентификации заключается в присвоении (выдаче) субъекту уникального идентификатора (идентификационного признака) для последующего сравнения его с имеющимся перечнем присвоенных идентификаторов. Каждый идентификатор характеризуется определенным уникальным двоичным кодом. В СКУД каждому коду ставится в соответствие информация о правах и привилегиях владельца идентификатора [2].

В ГОСТ Р 51241-2008«Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний» определены следующие виды идентификаторов, которые могут быть применены в СКУД:

- механические идентификаторы, использующие элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);
- магнитные идентификаторы, использующие намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т.д.);
- оптические идентификаторы, использующие нанесенные на поверхность или внутрь идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, топографические метки и т.д.);

- электронные контактные идентификаторы, использующие электронный код, записанный в электронной схеме идентификатора (дистанционные карты, электронные ключи и т.д.);
- акустические идентификаторы, использующие кодированный акустический сигнал;
- биометрические идентификаторы, использующие индивидуальные физические признаки человека (отпечатки пальцев, рисунок сетчатки глаза, динамика подписи и т.д.);
- комбинированные идентификаторы,использующие одновременно несколько идентификационных признаков.

На рис.1 представлены некоторые из перечисленных выше видов вещественных идентификаторов[3].

Рис. 1. Некоторые распространенные виды идентификаторов

Идентификация непосредственно связана с аутентификацией. Процедура аутентификации заключается в установлении подлинности предъявляемого субъектом идентификатора, что позволяет проверить, является ли идентифицирующийся субъект тем, за кого себя выдает. Аутентификация, в отличие от идентификации, подразумевает установление подлинности субъекта на основе сообщаемых им сведений о себе. Такие сведения называют аутентификаторами.

В зависимости от того, что предъявляется личностью в качестве аутентификатора, все существующие способы аутентификации личности можно разделить на следующие три классификационные группы:

- *по знанию*, основанные на наличии некоторой секретной информации, которую знает только аутентифицирующая себя личность, например, пароль, персональный идентификационный номер (ПИН), шифр замка, алгоритм, ответы на вопросы и т.п.;
- *по владению*, основанные на наличии некоторых физических предметов, которые могут быть предъявлены аутентифицирующей себя личностью, например, паспорт, пропуск, смарт-карта, токен (жетон) и т.п.;
- *по биометрии*, основанные на уникальных анатомических (статических) или поведенческих (динамических) отличительных характеристиках, которыми обладает аутентифицирующая себя личность, например, папиллярный рисунок пальцев рук (отпечатки пальцев), геометрия кисти руки, голос, почерк и т.п.

Способы аутентификации, представленные в каждой классификационной группе, имеют как преимущества, так и недостатки. Однако, биометрические системыаутентификации (БСА) по сравнению со средствами аутентификации «по знанию» и «по владению» имеют ряд преимуществ [4]:

- биометрические признаки трудно фальсифицировать;
- уникальность биометрических признаков обеспечивает высокую достоверность аутентификации;
- биометрические идентификаторы не могут быть забыты, потеряны или похищены, поскольку они являются неотъемлемой частью личности;
- использование в процедурах идентификации-аутентификации большинства биометрических идентификаторов удобно и комфортно для человека;

- использованиеряда биометрических идентификаторов (геометрия лица, геометрия кистей рук) позволяет проводить быструю и надежную идентификацию больших потоков людей.

В любых системах аутенфикации, включая и биометрические, представлены следующие два этапа использования:

- регистрация образа личности;
- аутентификация личности.

На первом этапе в системе выполняется регистрация всех личностей, подлежащих идентификации. Процедура регистрации производится путем первичных измерений биометрических характеристик личности, соответствующих типу БСА. Как правило, эти измерения выполняются несколько раз с последующим усреднением получаемых результатов. Затем из массива полученных результатов извлекается ограниченное число наиболее значимых свойств и на их основе формируется биометрический эталон – компактная машинная репрезентация биометрического образа личности. Биометрические эталоны личностей заносятся в специальную биометрическую базу данных (ББД) системы.

В начале этапа биометрической аутентификации также, как и на этапе регистрации, осуществляется измерение биометрических характеристик личности с целью формирования машинной репрезентации биометрического образа. Затем полученная машинная репрезентация биометрического образа сопоставляется с биометрическими эталонами, хранящимися в ББД системы.

Следовательно, любая БСА может быть представлена как система распознавания образов. Типовая структура БСА показана на рис. 2.

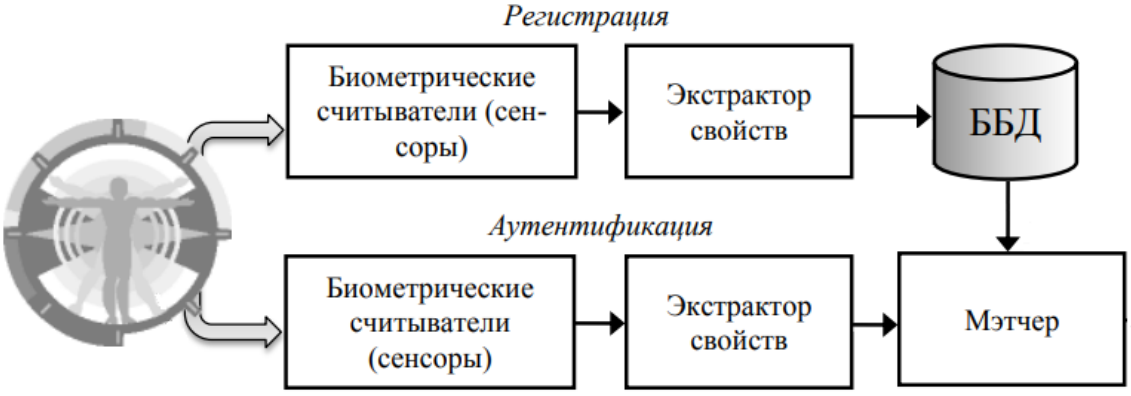

Рис. 2. Типовая структура БСА

БСА включает в себя следующие основные функциональные блоки [4]:

- Биометрические считыватели (сенсоры), осуществляющие измерение предъявляемых личностью биометрических данных соответствующей модальности.
- Экстрактор свойств, извлекающий значимые биометрические параметры из поступающих биометрических данных и формирующий их на основе машинную репрезентацию биометрического образа личности (биометрический эталон личности).
- Биометрическая база данных (ББД), хранящая биометрические эталоны всех зарегистрированных в системе личностей.
- Устройство сопоставления (мэтчер), осуществляющий сопоставление машинной репрезентации предъявленного биометрического образа личности с биометрическими эталонами, хранящимися в ББД.

Работа БСА осуществляется в двух режимах: регистрации и идентификации-аутентификации личности.Режим регистрации используется для создания биометрических эталонов личности всех пользователей системы. В этом режиме выполняется нормирование биометрических характеристик, представленных пользователем, затем с помощью экстрактора свойств извлекается значимая биометрическая информация, которая представляется в виде компактной машинной репрезентации, выполняющей роль биометрического эталона личности. При помощи некоторого дополнительного идентификационного параметра (учетного номера, логина, ПИН, пароля и т.п.) сформированный биометрический эталон связывается в единый массив с другими эталонами, хранящимися в ББД.

Режим идентификации-аутентификации является основным режимом БСА, котором осуществляется идентификация-аутентификация личности пользователя, предъявившего свои биометрические данные. В зависимости от используемого приложения в этом режимеБСА решаетследующие задачи: биометрическая верификация и биометрическая идентификация.

С позиции теории распознавания образов, задача биометрической верификации соответствует задаче классификации входных образов на два класса: «свой» и «чужой», т.е. сопоставление осуществляется по принципу 1:1. Задача биометрической идентификации соответствует задаче классификации входных образов на (m+1)классов, гдеm– число зарегистрированных в БСА пользователей («своих»), плюс один класс, включающий всех остальных, не зарегистрированных в БСА пользователей («чужих»), т.е. сопоставление осуществляется по принципу 1:m.

Биометрическая верификация – это процедура аутентификации личности пользователя, предъявившего БСА свои биометрические параметры и некоторый дополнительный, не биометрический идентификатор (логин, ПИН, пароль и т.п.). По этому идентификатору, выступающему в качестве адреса, БСА извлекает из ББД соответствующий биометрический эталон и сравнивает его с машинной репрезентацией предъявленного биометрического образа. Совпадение свидетельствует о том, что личность является той, за которую себя выдает.

БСА, реализующая режим биометрической верификации, может быть построена на основе как централизованной, так и распределенной ББД. В первом случае аутентифицирующийся субъект предъявляет свои биометрические характеристики, считываемые биометрическими сенсорам, на основе которых экстрактор формирует машинную репрезентацию в формате биометрических эталонов, хранящихся в централизованной ББД. Помимо биометрических характеристик субъект предъявляет также некоторый дополнительный идентификатор (логин, пароль, ПИН и т.п.), что позволяет БСА найти в ББД биометрический эталон, соответствующий данному субъекту. Далее мэтчер осуществляет сопоставление машинной репрезентации биометрических характеристик субъекта с биометрическим эталоном, извлеченным из ББД. В результате такого сопоставления получают ответ на вопрос – является ли данный субъект той личностью, за которую себя выдает. Следует отметить, что централизованные ББД в основном применяются в БСА, предназначенных для контроля логического доступа.

Во втором случае ББД представляет собой совокупность распределенных среди легальных субъектов персональных съемных носителей (смарт-карт, токенов и т.п.), содержащих биометрические характеристики своих владельцев. Субъект предъявляет БСА свои биометрические характеристики и съемный носитель, на котором записан его персональный биометрический эталон. Для инициирования транзакции требуется еще и дополнительный идентификатор, в качестве которого обычно используется ПИН. Мэтчер сопоставляет машинную репрезентацию биометрических характеристик, предъявленных субъектом, с его биометрическим эталоном, считанным с носителя. В результате сопоставления получают ответ на вопрос – является ли данный субъект той личностью, за которую себя выдает. При этом обмен информацией между БСА и съемным носителем, содержащим эталон,осуществляется по безопасному протоколу.

Распределенные ББД получили преимущественное распространение в БСА, предназначенных для контроля физического доступа в помещения и на территории охраняемых объектов. Во многих БСА применяются ББД обоих типов. При этом распределенная ББД используется для ежедневной офлайн-верификации субъекта, а централизованная ББД – для онлайн-верификации или для перевыпуска съемных носителей, в случае их утраты, без повторного снятия биометрических характеристик субъекта.

Биометрическая идентификация – это процедура аутентификации личности пользователя исключительно на основе предъявленных им биометрических параметров. В этом случае БСА поочередно сравнивает машинную репрезентацию предъявленного биометрического образа с биометрическими эталонами всех зарегистрированных в БСА пользователей. Результатом сравнения является получение ответа на вопрос – зарегистрирован данный пользователь в БСА или нет.

В режиме биометрической идентификации субъект предъявляет свои биометрические характеристики, которые считываются с помощью биометрических сенсоров, экстрактор свойств формирует из них машинную репрезентацию в формате биометрических эталонов, хранящихся в ББД. Мэтчер инициирует процедуру поочередного сопоставления предъявленной машинной репрезентации с каждым биометрическим эталоном ББД. Результатом этой является список идентификаторов, имеющих наибольшую степень сходства с предъявленной репрезентацией. Возможен также отрицательный ответ, свидетельствующий об отсутствии в ББД идентификаторов, обладающих достаточным сходством с предъявленным идентификатором.

Существуют следующие два варианта реализации режима биометрической идентификации:

- Положительная идентификация, при которой БСА определяет, зарегистрирован ли данный субъект в ББД. При этом могут быть допущены ошибки ложного отказа доступа и ложного доступа.
- Отрицательная идентификация, при которой БСА проверяет факт отсутствия образа субъекта в ББД. При этом могут быть допущены ошибки ложного признания и ложного отрицания.

Процедура биометрической аутентификации всегда регламентируется аутентификационными протоколами, определяющими последовательность шагов по решению задачи идентификации-аутентификации в БСА.

Аутентификационный протокол – это (автоматизированный)процесс принятия решения, действительно ли удостоверяющие данные субъекта являются достаточными для подтверждения его личности, чтобы разрешить ему доступ на основе этих удостоверяющих данных или других признаков.

Любой аутентификационный протокол, использующий различные методы (и разные биометрические идентификаторы), может быть определен и выполнен на основе представленных удостоверяющих данных [5].

Использование технологии систем контроля и управления доступом по биометрии (БиоСКУД) становится все более популярным как в государственных структурах, так и в коммерческих организациях (офисных центрах, промышленных и торговых предприятиях, фитнес-клубах и др.).

Одним из основных преимуществ технологии БиоСКУД является ее надежность, поскольку биометрические данные являются уникальными для каждого человека и их невозможно потерять (в отличие от карт доступа или паролей, которые могут быть похищены, подделаны или подобраны). Автоматическая работа БиоСКУД позволяет исключить риски несанкционированного пропуска некоторого лица сотрудниками охраны. Кроме того, БиоСКУД позволяет существенно сократить время на проход (например, человеку не нужно искать карту или вводить парольдоступа, а достаточно лишь взглянуть в камеру для распознавания лица) [6].

В настоящее время применение БиоСКУД регламентируется Федеральным законом от 29.12.2022 №572-ФС «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации». В качестве государственной цифровой платформы, позволяющей подтвердить личность человека по его биометрическим характеристикам, выступает Единая биометрическая система (ЕБС). Функции оператора ЕБС возложены на Центр Биометрических Технологий (АО «ЦБТ»).

Список литературы

1. Козлов, А. Е. Система контроля и управления доступом на предприятие: понятие, характеристика и основные требования / А. Е. Козлов //

Вестник Воронежского государственного технического университета. Т. 15. №1. 2019. – С. 42- 47.

2. Ворона, В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. –М. : Горячая линия-Телеком, 2010. –272 с. – ISBN 978-5-9912-0059-2.

3. Михайлов А. Комплексный подход при идентификации личности / А. Михайлов, А. Колосков, Ю. Дронов // Системы безопасности. 2015.№4. – С. 62-71.

4. Брюхомицкий, Ю. А. Биометрические технологии идентификации личности : учебное пособие / Ю. А. Брюхомицкий; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Изд-во ЮФУ, 2017. – 263 с. – ISBN 978-5-9275-2454-9.

5. Соколов, Д. В. Понятие «Биометрия». Биометрические аутентификационные протоколы / Д. В. Соколов // Безопасность информационных технологий. 2012. №3.– С. 70-74.

6. Чеботарев П. БиоСКУД: перезагрузка и новые требования / П. Чеботарев // Системы безопасности. 2023. №6.

References

1. Kozlov, A. E. Access control and management system for the enterprise: concept, characteristics and basic requirements / A. E. Kozlov // Vestnik of Voronezh State Technical University. T. 15. No. 1. 2019. - pp. 42-47.

2. Vorona, V. A. Systems of access control and management / V. A. Vorona, V. A. Tikhonov. -M. : Hotline-Telecom, 2010. -272 p. - ISBN 978-5-9912-0059-2.

3. Mikhailov, A. A complex approach to personal identification / A. Mikhailov, A. Koloskov, Y. Dronov // Security Systems. 2015.№4. - pp. 62-71.

4. Bryukhomitskiy, Y. A. Biometric technologies of personal identification: textbook / Y. A. Bryukhomitskiy; Southern Federal University. - Rostov-on-Don; Taganrog: Izd-vo YFU, 2017. - 263 p. - ISBN 978-5-9275-2454-9.

5. Sokolov, D. V. The concept of "Biometrics". Biometric authentication protocols / D. V. Sokolov // Security of information technologies. 2012. No. 3.- pp. 70-74.

6. Chebotarev P. Biosecurity: reboot and new requirements / P. Chebotarev // Security Systems. 2023. No. 6.