УДК 004.5.

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ОСНОВЕ ИНТЕГРАЛЬНЫХ ПАРАМЕТРОВ

Д.т.н. И.Ш. Невлюдов, к.т.н. А.В. Пономарева, В.О. Бортникова, А.А. Мордик, Харьковский национальный университет радиоэлектроники

В статье проанализирована современная структура систем контроля и управления доступом (СКУД). Сформулирована их обобщенная структурная схема. Предложено использовать методы машинного обучения для интеллектуализации СКУД, сформированы интегральные параметры и произведена постановка задачи исследования.

У статті проаналізовано сучасну структура систем контролю і управління доступом (СКУД). Сформульована їх узагальнена структурна схема. Запропоновано використовувати методи машинного навчання для інтелектуалізації СКУД, сформовані інтегральні параметри і проведена постановка задачі дослідження.

The modern structure of access monitoring and control system (AMCS) was analyzed. Their generalized structure was formulated. The methods of machine learning are proposed to use for intellectualization of AMCS, integral parameters formed and setting of the study performed.

Ключевые слова: *СКУД, автоматизация, машинное обучение, классификация*

Введение

Для обеспечения охраны и защиты объектов будь то предприятие, завод, ВУЗ существует огромное множество технических средств и систем, которые должны обеспечивать надежную охрану и защиту комплекса имеющихся на предприятии ресурсов от комплекса возможных угроз с минимально возможными затратами, не превышающими 20% стоимости защищаемых ресурсов [1].

На сегодняшний день трудно представить крупное промышленное предприятие, офис, банк, учебное заведение без современных систем контроля и управления доступом (СКУД). В последнее время все большее значение получили автоматизированные системы контроля и управления доступом. Одними из наиболее перспективных считаются бесконтактные СКУД. В основе их работы заложена идея определения сотрудника или пользователя по какому-либо признаку или устройству, благодаря которому происходит верификация и идентификация персонала [2].

СКУД играют важную роль в обеспечении безопасности любой организации, а использование интеллектуальных автоматизированных СКУД на предприятии несомненно приводит к повышению качества, обеспечению повышения уровня безопасности и защищенности, позволяет ограничить доступ посторонним лицам, вести учет перемещения сотрудников на предприятии и адаптироваться к изменяющимся внешним условиям. Таким образом, разработка новых подходов и алгоритмов решения задачи интеллектуализации СКУД является актуальной задачей.

Анализ структуры систем контроля и управления доступа

СКУД в общем случае представляет собой объединенные в комплексы электронные, механические, электротехнические, аппаратно-программные и иные средства, обеспечивающие возможность доступа определенных лиц в определенные зоны (территория, здание, помещение) или к определенной аппаратуре, техническим средствам и предметам (ПК, автомобиль, сейф и т. д.) и ограничивающие доступ лицам, не имеющим такого права [3].

Упомянутые системы могут осуществлять контроль перемещения людей и транспорта по территории предприятия, обеспечивать безопасность персонала и посетителей, а также сохранность материальных и информационных ресурсов предприятия.

СКУД классифицируют по следующим категориям [4]:

- по способу управления;
- числу контролируемых точек доступа;
- функциональным характеристикам;
- виду объектов контроля;
-уровню защищенности системы от несанкционированного доступа.

Кроме того, все СКУД делятся на четыре класса [5]:

- СКУД 1-го класса – малофункциональные системы малой емкости, работающие в автономном режиме и осуществляющие допуск всех лиц, имеющих соответствующий идентификатор. В такой системе используется ручное или автоматическое управление исполнительными устройствами, а также световая или/и звуковая сигнализация.

- СКУД 2-го класса – монофункциональные системы. Они могут быть одноуровневыми и многоуровневыми и обеспечивают работу как в автономном, так и в сетевом режимах. Допуск лиц (групп лиц) может осуществляться по дате, временным интервалам. Система способна обеспечить автоматическую регистрацию событий и автоматическое управление исполнительными устройства.

- СКУД 3-го и 4-го классов, как правило, являются сетевыми. В них используются более сложные идентификаторы и различные уровни сетевого взаимодействия (клиент-сервер, интерфейсы считывателей карт Виганда или магнитных карт, специализированные интерфейсы и др.).

СКУД содержит 4 основных элемента: идентификатор пользователя (карта-пропуск, ключ),

устройство идентификации, управляющий контроллер и исполнительные устройства.

Также современные СКУД можно классифицировать по типу оборудования (на базе терминалов доступа, на базе контроллеров доступа и считывателей, на базе автономных электронных замков), по типу идентификатора (бесконтактная карта, код доступа, отпечаток пальца, образ лица, мультиидентификация), по типу программирования (автономные – программирование устройства возле точки прохода с помощью мастер карты, сетевые – создание сети устройств доступа под управлением одного программного обеспечения, универсальные – сочетают возможности автономных и сетевых систем), по типу сетевых интерфейсов (RS485, Ethernet, WiFi, GPRS), по условиям применения (для внутреннего применения, для улицы).

Обобщенная структурная схема интеллектуальной автоматизированной СКУД

Проведя анализ различных современных СКУД [13-19], разработана обобщенная структурная схема, представленная на рисунке 1.

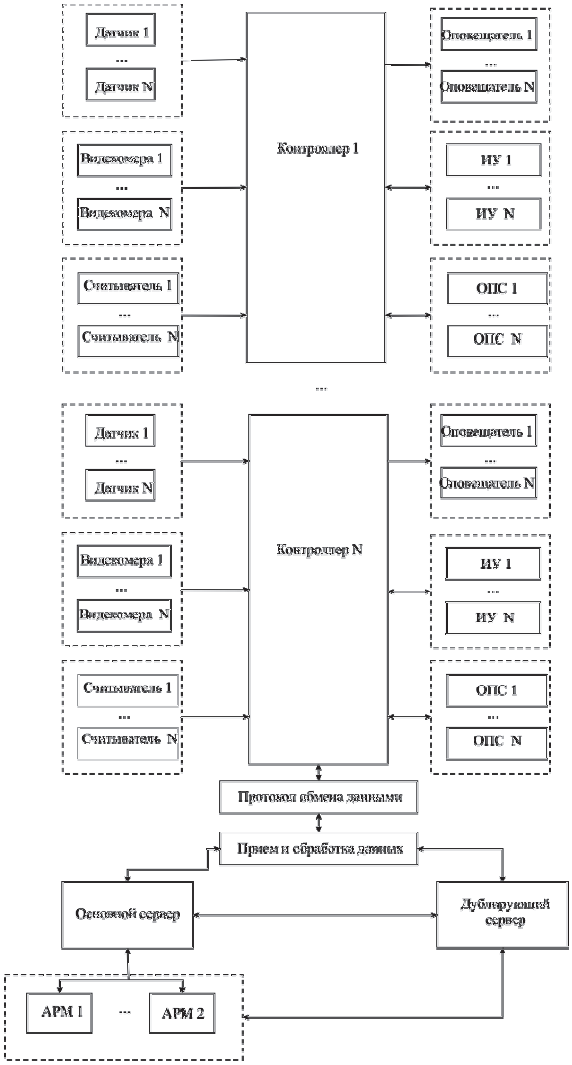

Рис. 1. Обобщенная структурная схема автоматизированной СКУД

Структурная схема, включает в себя такие элементы.

- датчики (датчики открытия\закрытия двери, датчики движения, разбития, присутствия, датчик состояния двери и т.д.);
- видеокамеры и видеорегистраторы;
- считыватели ключей;
- оповещатели (световые, звуковые или комбинированные);
- исполняющие устройства (ИУ) (турникеты, замки, защелки, герконы и т.д.);
- охранно-пожарную сигнализацию (ОПС);
- контроллеры СКУД;
- серверы (основной и дублирующий);
- автономные рабочие места (АРМ) (пост охраны, администратора СКУД и т.д.).

Необходимо учесть, что СКУД может иметь не все предложенные элементы, а их выбор зависит от поставленной задачи.

Известно, что важным элементом СКУД является обеспечение возможности комплексной идентификации пользователя по нескольким признакам. К таким признакам относится не только электронный пропуск, но и биометрические показатели (отпечаток пальца, лицо, радужная оболочка глаза, по геометрии руки, по термограмме лица, по ДНК, на основе акустических характеристик уха, по рисунку вен, по почерку, голосу, походке и др.), автомобильный номер и т.д. Большинство СКУД задачу биометрической идентификации возлагает на субъективное мнение оператора. Таким образом, сегодня предприятия обладает повышенными требованиями к СКУД, а как следствие имеют потребность в многофакторной аутентификации.

Одним из ключевых факторов работы таких сложных СКУД является обеспечение быстродействия системы. Длительный период распознавания будет создавать очередь перед проходной. Время прохода через турникет и проходную складывается из сканирования данных, обработки и передачи данных на сервер, получения шаблона, сравнения шаблона с полученными данными, открытие турникета, двери, проходной.

Для того чтобы автоматизировать СКУД и обеспечить безопасность ее работы необходимо иметь базу данных с записанными данными сотрудников (фотографией, ФИО и другими параметрами), постоянно ее обновлять и модернизировать.

На сегодняшний день большую популярность приобрели СКУД с распознаванием лиц сотрудников, обеспечивая высокий процент распознавания. Обычно заказчик настаивает на проценте не ниже чем 99% [20].

Для достижения такого высокого показателя необходимо сделать фото одной камерой, однако в реальности чаще всего это представляется возможным из-за различного места установки камер, разного освещение точек прохода. Вследствие чего хранят и используют для распознавания адаптивные шаблоны лица для каждого сотрудника и для каждой видеокамеры в отдельности.

Еще одним не мало важным параметром, которым должна отвечать интеллектуальная СКУД – число лиц в базе данных. Увеличение численности пользователей в

системе не должно отражаться на времени поиска и, как следствие, времени прохода, а, следовательно, такая система должна иметь быстрые алгоритмы идентификации и аутентификации.

Методы машинного обучения для решения задачи идентификации сотрудника

Представленный подход к созданию интеллектуальной СКУД базируется на интегральном показателе описательных признаков каждого сотрудника, который включает в себя не только информацию о персональных данных, номера ID-ключа, но и шаблон биологических признаков сотрудника.

Учитывая, что человек изменяется как с возрастом, так и сменой времен года, погодных условий, можно столкнуться с проблемой снижения вероятности правильной идентификации сотрудника. Таким образом, необходимо разработать такой подход к обучению интеллектуальной системы идентификации личности, который позволит с течением времени автоматически модифицировать и заменять/добавлять новые признаковые описания в шаблоне признаков сотрудника.

Одним из наиболее эффективных способов является режим «машинного обучения», при котором набор признаков о сотруднике попадает в базу данных и анализируется автоматически, при каждом прохождении контрольного пункта. При первом поднесении персональной карты производится регистрация и формирование шаблона признаков для верификации человека (процедура обучения компьютерной системы).

Принципы машинного обучения позволяют анализировать, учитывать большое количество разнотипных входных данных и достигать высокого качества работы алгоритмов, обеспечивая высокую скорость обработки данных. Задача идентификации сотрудников по различным признакам можно свести к задачи классификации.

Предположим, что существует множество допустимых описаний сотрудника P, а A множество всех сотрудников. Тогда можно записать целевую функцию:

$$P^* : P \to A \ , \qquad (1)$$

где $P_i = P_i^*(a_i)$ – значения целевой функции, известно на конечном множестве сотрудников $\{a_1, a_2, \dots a_x\} \subset A$.

Совокупность пар «описание-сотрудник» $P^x = (p_i, a_i)_{i=1}^x$ будем называть обучающей выборкой.

Признаком λ, описывающим сотрудника, назовем такое отображение:

$$\lambda : A \to F_\lambda \ , \qquad (2)$$

где F_λ – множество допустимых значений признака.

Зададим признаки сотрудников $\lambda_1, \lambda_2, \dots \lambda_n$, тогда вектор $(\lambda_1(p), \lambda_2(p), \dots \lambda_n(p))$ называется признаковым описанием сотрудника $p \in P$.

Следовательно, для каждого сотрудника $\{a_1, a_2, \dots a_x\} \subset A$ существует вектор его признакового описания $(\lambda_1(p), \lambda_2(p), \dots \lambda_n(p))$. Объединив совокупность признаковых описаний всех сотрудников выборки P^x запишем ее в виде матрицы размерностью $x \times n$:

$$\begin{pmatrix} \lambda_1(p_1) & \dots & \lambda_n(p_1) \\ \lambda_1(p_1) & \dots & \lambda_n(p_1) \\ \dots\dots\dots\dots\dots\dots & & \\ \lambda_1(p_x) & \dots & \lambda_n(p_x) \end{pmatrix},$$

где каждая строка матрицы – вектор параметров x-го сотрудника.

Вектор признаковых описаний сотрудника будет содержать в себе такие интегральные параметры как:

$$\lambda_n = \{\Xi_j, m_j, \psi_j, RF_j, \theta_j\}, \qquad (3)$$

где Ξ_j – вектор параметров, полученных с камер видеонаблюдения (изображение в интегральном представлении, признаки Хаара) [15];

m_j – вектор метрических параметров (вес, рост и т.д.)

ψ_j – вектор персональных данных сотрудника (Ф.И.О. сотрудника, отдел, должность и т.п.);

RF_j – идентификатор метки электронного ключа;

θ_j – дополнительные признаки, необходимы для идентификации и аутентификации сотрудника.

Учитывая, что задача идентификации сотрудника A относится к классификации непересекающихся классов. Тогда необходимо множество описание допустимых признаков сотрудника P разбить на классы:

$$Cl_A = \{p \in P : a^*(p) = A\} \ . \qquad (4)$$

Решением поставленной задачи будет ответ на вопрос к какому классу Cl_A принадлежит сотрудник A и является ли это соответствие истинной.

При автоматическом принятии решения о предоставлении доступа сотруднику с использованием предложенного метода необходимо учитывать особенности практической реализации: недостаточный объем выборки, возможные «пропуски» данных (связано с несовершенством технических средств и алгоритмов получения биометрических данных с изображения), необходимость разработки интерпретируемого алгоритма классификации и оценка вероятности модели машинного обучения.

Выводы

В работе усовершенствована система контроля и управления доступом в помещение с использованием компьютеризированных технологий и методов машинного обучения. Предложена обобщенная структурная схема интеллектуальной СКУД, которая кроме традиционных элементов СКУД включает программно-аппаратные решения для идентификации личности. Анализ интегрального показателя описательных признаков каждого сотрудника, который включает в себя информацию о персональных данных, номера ID-ключа, шаблон его биологических признаков, и использование методов машинного обучения повышает уровень надежности СКУД и эффективности идентификации личности.

Для практической реализации предложенного подхода необходимо разработать алгоритм машинного обучения для реальных выборок, выбрать метод оценки эффективности предложенного алгоритма.

СПИСОК ЛИТЕРАТУРЫ:

1. Волхонский, В.В. Системы контроля и управления доступом - Санкт-Петербург: СПб: Университет ИТМО, 2015. - 105 с.

2. Руководство по составлению спецификаций на СКУД/ Британская Ассоциация индустрии безопасности. – Security Focus, 2014. – 170 С.

3. Петин, В.А. Проекты с использованием контроллера Arduino/ В.А. Петин. – Москва: "БХВ-Петербург ", 2014. – 241 с.

4. Ворона, В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов – М.: Горячая линия-Телеком, 2010. – 272 с.

5. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. – Москва: Изд-во стандартов, 2009. – 32 с.

6. Алешин, А. П. Техническое обеспечение безопасности бизнеса / А. П. Алешин. – М.: Дашков и Ко, 2008 г. – 160 с.

7. ISO/IEC 7810:2003 Identification cards – Physical characteristics. – 2015. – 11 p.

8. Смарт-карта [Электронный ресурс]// URL:http://dengi.polnaya.info/platezhnye_sistemy/smart_karta/ (дата обращения: 21.09.2016).

9. Финкенцеллер, К. Справочник по RFID. Теоретические основы и практическое применение индуктивных радиоустройств, транспондеров и бесконтактных чип-карт. / К. Финкенцеллер. – Додэка, 2008. – 496 с.

10. Новый обзор электронных ключей-идентификаторов [Электронный ресурс]// URL: http://www.gaw.ru/html.cgi/txt/publ/other/ibutton.htm (дата обращения: 25.09.2016).

11. Считыватель RFID RC522 [Электронный ресурс]// URL: http://arduino-kit.ru/userfiles/image/RFIDRC522.pdf (дата обращения: 02.10.2016).

12. Чтение и запись RFID меток. Модуль RC522 для Arduino. URL: http://arthurphdent.livejournal.com/1759.html (дата обращения: 04.11.16).

13. СКУД Anvi [Электронный ресурс]// URL: http://anviz.ru/systems/acs.html (дата обращения: 23.10.2016).

14. Интеллектуальный СКУД "СФИНКС"[Электронный ресурс]// URL: http://ipstm.ru/produkciya/intellektualnyy-skud-sfinks (дата обращения: 23.10.2016).

15. Система контроля и управления доступом «ПОСТ СКУД» [Электронный ресурс]// URL: http://in-tex.ru/production-cat15/ (дата обращения: 23.10.2016).

16. Архив записей – СКУД [Электронный ресурс]// URL: http://int-sys.ru/tag/skud/ (дата обращения: 23.10.2016).

17. Система контроля и управления доступом Neuroniq [Электронный ресурс]// URL: http://neuroniq.ru/neuroniq/sistema-kontrolya-i-upravleniya-dostupom/ (дата обращения: 23.10.2016).

18. Биометрический СКУД CASTLE [Электронный ресурс]// URL: http://www.agrg.ru/castle/bio (дата обращения: 23.10.2016).

19. Биометрический СКУД BioSmart [Электронный ресурс]// URL:http://basb.ru/biometricheskaya-sistema-kontrolya- (дата обращения: 23.10.2016).

20. Особенности внедрения и использования систем контроля доступа по лицу [Электронный ресурс]// URL:http://www.secuteck.ru/articles2/sys_ogr_dost/osobennosti-vnedreniya-i-ispolzovaniya-sistem-kontrolya-dostupa-po-litsu/ (дата обращения: 23.10.2016).

21. Биометрическая идентификация и аутентификация [Электронный ресурс]// URL:http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html (дата обращения: 23.10.2016).

22. Вьюгин В.В. Математические основы теории машинного обучения и прогнозирования/ В.В. Вьюгин. - М.: 2013. - 387 с.

23. Вьюгин В.В. Элементы математической теории машинного обучения: учеб. пособие. – М.: МФТИ: ИППИ РАН, 2010. – 231с.

24. Воронцов К.В. Машинное обучение, лекции [Электронный ресурс]// URL: http://www.machinelearning.ru/wiki/images/6/6d/Voron-ML-1.pdf (дата обращения: 17.11.16).

25. Дьяконов А.Г. Практикум на ЭВМ кафедры математических методов прогнозирования (системы WEKA, RapidMiner и MatLab): Учебное пособие. – М.: Издательский отдел факультета ВМиК МГУ им. М.В. Ломоносова; МАКС Пресс, 2010. – 133с.

26. Наумов Н. Разработка метод Виолы-Джонса (Viola-Jones) как основа для распознавания лиц [Электронный ресурс]// URL: https://habrahabr.ru/post/133826/(дата обращения: 17.11.16).

27. Золотых Н.Ю. Учебные материалы по машинному обучению [Электронный ресурс]// URL: http://www.uic.unn.ru/~zny/ml/ (дата обращения: 17.11.16)