DOI 10.21672/2074-1707.2021.53.1.083-090
УДК 004.89

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ ЛИЦ В СИСТЕМАХ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Статья поступила в редакцию 15.12.2020, в окончательном варианте – 17.01.2021.

Марьенков Александр Николаевич, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
кандидат технических наук, заведующий кафедрой информационной безопасности и цифровых технологий, ORCID https://orcid.org/0000-0003-1378-3553, e-mail: marenkovan17@gmail.com
Кузнецова Валентина Юрьевна, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
ассистент кафедры информационной безопасности и цифровых технологий, ORCID https://orcid.org/0000-0002-6954-5020, e-mail: arhelia@bk.ru
Гелагаев Тимур Магомедович, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
студент, e-mail: tgelagaev@yandex.ru

В статье показана актуальность повсеместного использования технологии компьютерного зрения на примере распознавания лиц в рамках системы контроля и управления доступа. Рассмотрены основные методы, которые применяются при реализации классических систем контроля и управления доступом. Описана схема реализации пропускного режима с технологией распознавания лиц. Применение данной технологии позволяет повысить уровень информационной безопасности предприятий и, как следствие, снизить возможный финансовый ущерб от реализации атак на их активы от нелегитимного проникновения на защищаемую территорию через СКУД с помощью пропусков легальных пользователей.
Ключевые слова: система контроля и управления доступом, распознавание лиц, нейронные сети, безопасность, пропускной режим

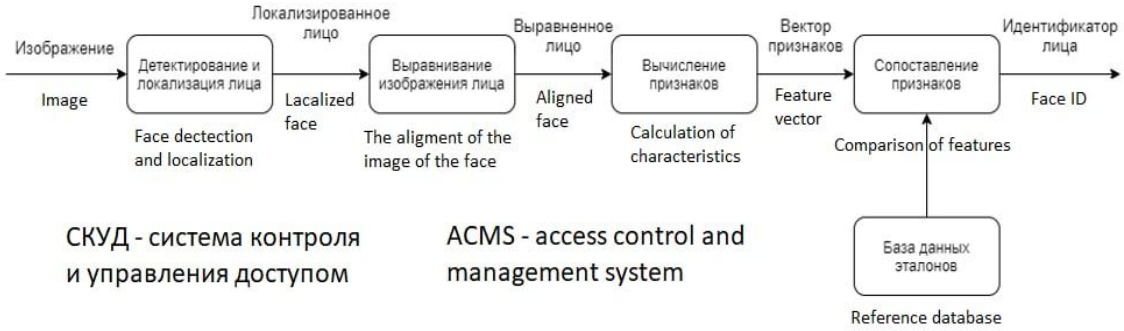
APPLICATION OF FACE RECOGNITION TECHNOLOGIES IN CONTROL AND ACCESS CONTROL SYSTEMS

The article was received by the editorial board on 15.01.2021, in the final version – 17.02.2021.

Marenkov Alexander N., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Cand. Sci. (Engineering), Head of the Department of Information Security and Digital Technologies, ORCID https://orcid.org/0000-0003-1378-3553, e-mail: marenkovan17@gmail.com
Kuznetsova Valentina Yu., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
assistant of the Department of Information Security and Digital Technologies, ORCID https://orcid.org/0000-0002-6954-5020, e-mail: arhelia@bk.ru
Gelagaev Timur M., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
student, e-mail: tgelagaev@yandex.ru

The article shows the relevance of the widespread use of computer vision technology on the example of face recognition as part of the access control and management system. The main methods that are used in the implementation of classical control systems and access control are considered. The scheme for the implementation of the access control with face recognition technology is described. The use of this technology makes it possible to increase the level of information security of enterprises and, as a result, reduce the possible financial damage from the implementation of attacks on their assets from illegitimate penetration into the protected area through the access control system using the passes of legal users.
Keywords: access control and management system, face recognition, neural networks, security, access control

Graphical annotation (Графическая аннотация)



Введение. Использование компьютерного зрения в области обеспечения безопасности даёт огромный толчок к совершенствованию систем контроля и управления доступом (СКУД). Представители среднего и крупного бизнеса, использующие СКУД на своих объектах, приводят информацию о том, что каждый пятидесятый проход через турникет осуществляется с нарушением требований безопасности – для проникновения на территорию с ограниченным доступом используются карты легальных пользователей или поддельные карты доступа. Технологии распознавания лиц планомерно внедряются во многие технологические процессы, в том числе и в системы обеспечения безопасности. СКУД с использованием технологии распознавания лиц способствует детектированию ситуаций, когда для прохода злоумышленник применяет карту легального пользователя путем сравнения лица владельца карты из базы данных организации с портретом того, кто пытается проникнуть на охраняемую территорию. Усовершенствование СКУД таким образом позволит повысить уровень информационной безопасности предприятий и, как следствие, снизить возможный финансовый ущерб от реализации атак на их активы. Кроме того, бесконтактная идентификация пользователей путем распознавания их лиц актуальна в условиях неблагоприятной эпидемиологической обстановки.

Принцип работы классической СКУД. Система контроля и управления доступом – одна из наиболее популярных и эффективных систем защиты территории с ограниченным доступом. СКУД ограничивает проход на охраняемую территорию, при этом никаким образом не вмешиваясь в бизнес-процессы организации. Кроме того, система обеспечивает отслеживание перемещений сотрудников внутри организации и учёт их отработанного времени, что способствует нарушению трудового распорядка.

Основные функции:

- ограничение доступа к помещениям охраняемого объекта;
- ведение табельного учета рабочего времени для каждого сотрудника;
- фиксирование времени прихода и ухода посетителей;
- персональный и временной контроль за открытием внутренних помещений;
- контроль за перемещениями сотрудников по объекту;
- регистрация и уведомление о случаях попыток проникновения в охраняемые помещения;
- интеграция и взаимодействие между системами видеоконтроля и охранно-пожарной сигнализации.

Классический принцип работы СКУД заключается в следующем: она представляет собой пропускную систему на основе ключ-карт с RFID-метками.

Аббревиатура RFID образована от термина Radio Frequency Identification, что в переводе на русский означает «радиочастотная идентификация». RFID-метка состоит из трёх компонентов:

- чип, который хранит идентификационную информацию и отвечает за связь со считывателем;
- антенна, позволяющая передать информацию между меткой и считывателем;
- оболочка или корпус.

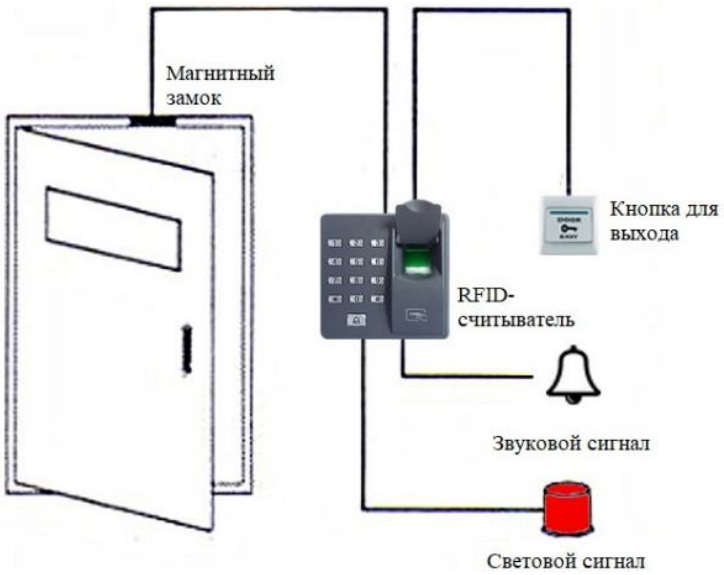


Рисунок 1 – Классическая схема СКУД на предприятии

В настоящее время системы RFID можно встретить абсолютно везде, начиная с общественного транспорта (оплата проезда посредством карты, привязанной к счёту пользователя), проживания в отеле (смарт-карта является ключом для входа в номер) заканчивая заграничным паспортом (нового поколения), который можно получить с электронным бесконтактным RFID-чипом [3].

Практика показывает, что такой вид контроля управления доступом имеет ряд недостатков, которые могут провоцировать уязвимости, связанные с несанкционированным доступом к информационным ресурсам охраняемого объекта. Наиболее ярким примером такого недостатка является использование чужих карт для прохода на охраняемую территорию, например, такое возможно, если сотрудник забыл карту дома и попросил своего коллегу «одолжить» ему карту для прохода, либо, что хуже, потерянную или выкраденную карту использовал для прохода злоумышленник.

Также существенной проблемой для СКУД является распространившееся клонирование ключей и карт доступа. В прессе и на сайтах объявлений часто можно увидеть информацию об услугах по клонированию ключей доступа для любого желающего, например, за такой услугой часто обращаются пользователи домофонов. Однако использование таких ключей в СКУД значительно снижает эффективность при обеспечении безопасности в организации. Многие СКУД не препятствуют одновременному использованию нескольких одинаковых ключей или карт доступа. Клонированный ключ позволяет не только пройти на предприятие, но также открывает все внутренние двери, которые были разрешены для аутентичного ключа.

Чаще всего данную проблему решают с помощью установки биометрических сканеров (отпечатки пальцев, сетчатки глаза и пр.), однако в условиях неблагоприятной эпидемиологической ситуации данные системы становятся все менее востребованными. При этом бесконтактные системы считывания отпечатков пальцев показывают низкую результативность. Согласно отчету американского национального института стандартов и технологий (NIST), точность бесконтактных устройств при распознавании одного пальца была относительно низкой – всего 60–70 %.

Распознавание лиц в целях обеспечения безопасности. Распознавание лиц – это одни из наиболее перспективных методов биометрической бесконтактной идентификации человека по лицу. Согласно прогнозам аналитиков Future Market Insights, мировой рынок бесконтактных биометрических технологий в период с 2020 по 2030 годы будет расти среднегодовыми темпами на уровне 17,4 % и к 2030 году достигнет $70 млрд. Ожидается, что бесконтактная технология будет более востребована из-за пандемии коронавируса в мире и проблем гигиены поверхностей, таких как контактные сканеры отпечатков пальцев [4].

Распознавание лица представляет собой процесс сопоставления изображений лиц людей, попавших в объектив камеры с фотографиями из базы данных ранее сохраненных изображений лиц эталонов, например сотрудников организации. По структурной реализации системы распознавания лиц выделяют 3 схемы:

1. Анализ видеопотока на сервере: IP-камера направляет весь видеопоток на сервер для обработки и анализа. На сервере специализированное программное обеспечение выполняет поиск лица в видеоряде и сравнивает полученные из видеопотока изображения лиц с базой лиц эталонов (рис. 2).

Рисунок 2 – Схема анализа видеопотока на сервере

Недостатками такой схемы будут высокая нагрузка на сеть, высокая стоимость сервера, даже к самому мощному серверу можно подключить ограниченное количество IP-камер, т.е. чем больше система, тем больше серверов. Преимуществом является возможность использовать существующую систему видеонаблюдения.

2. Анализ видеопотока на IP-камере: изображения будут производиться на самой камере, а на сервер будут передаваться обработанные метаданные (рис. 3).

Рисунок 3 – Схема анализа видеопотока на камере

Недостатки – нужны специальные камеры, выбор которых в данный момент крайне мал, стоимость камер выше, чем у обычных. Также в системах разных производителей будет по-разному решаться вопрос хранения и размера базы данных распознанных лиц эталонов, а также вопросов взаимодействия софта на камере и софта на сервере.

Преимущества – подключение практически неограниченного количества камер к одному серверу.

3. Анализ видеопотока на устройстве контроля доступа – камера встроена в устройство контроля доступа, которое кроме распознавания лица, происходящего на устройстве, выполняет функции управления доступом, как правило, через турникет или электрозамок, установленный на дверь (рис. 4). База данных лиц эталонов хранится на устройстве, и уже не в виде фотоизображений.

Рисунок 4 – Анализ видеопотока на устройстве контроля доступа

Недостатки – как правило, все такие устройства выпускаются для использования в помещениях. Преимущества – низкая стоимость систем по сравнению с системами видеонаблюдения, используемыми для распознавания лиц.

Как правило, все предлагаемые методы распознавания лиц реализуются преимущественно с помощью 2D-изображений, так как, несмотря на развитие трехмерных моделей, база таких эталонов еще достаточно скудная, а оборудование для организации такого рода распознавания является дорогостоящим.

Анализ подходов распознавания лиц. Несмотря на разнообразие существующих подходов, можно определить общий алгоритм распознавания лиц, представленный на рисунке 5.

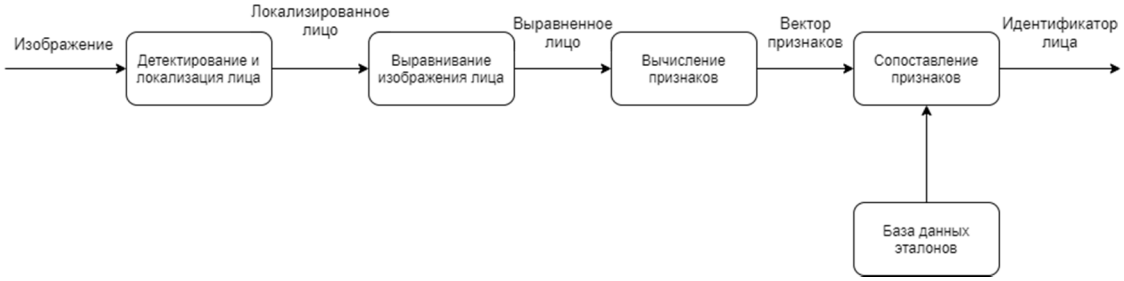


Рисунок 5 – Общая схема алгоритма распознавания лиц

Основным этапом описываемого процесса является само распознавание лица, которое обеспечивается за счет вычисления признаков и выявления схожести или несхожести фотографий. Рассмотрим несколько методов, которые могут быть применены в алгоритме распознавания лиц.

Метод гибкого сравнения на графах. Суть этого метода сводится к сопоставлению графов. Лица представляются в виде графов со взвешенными вершинами и ребрами. На этапе распознавания один из графов – эталонный – остается неизменным, в то время как другой изменяется с целью наилучшей подгонки к первому. В подобных системах распознавания графы могут представлять собой как прямоугольную решетку, так и структуру, образованную характерными (антропометрическими) точками лица. Различие (расстояние) между двумя графами вычисляется при помощи некоторой ценовой функции деформации, учитывающей как различие между значениями признаков, вычисленными в вершинах, так и степень деформации ребер графа.

Нейронные сети. В настоящее время существует около десятка разновидности нейронных сетей (НС). Обучаются нейронные сети на наборе обучающих примеров. Суть обучения сводится к настройке весов межнейронных связей в процессе решения оптимизационной задачи методом градиентного спуска. В процессе обучения НС происходит автоматическое извлечение ключевых признаков, определение их важности и построение взаимосвязей между ними. Предполагается, что обученная НС сможет применить опыт, полученный в процессе обучения, на неизвестные образы за счет обобщающих способностей. Наилучшие результаты в области распознавания лиц (по результатам анализа публикаций) показала сверточная нейронная сеть.

Скрытые Марковские модели. Одним из статистических методов распознавания лиц являются скрытые Марковские модели (СММ) с дискретным временем. СММ используют статистические свойства сигналов и учитывают непосредственно их пространственные характеристики. Элементами модели являются: множество скрытых состояний, множество наблюдаемых состояний, матрица переходных вероятностей, начальная вероятность состояний. Каждому соответствует своя Марковская модель. При распознавании объекта проверяются сгенерированные для заданной базы объектов Марковские модели и ищется максимальная из наблюдаемых вероятность того, что последовательность наблюдений для данного объекта сгенерирована соответствующей моделью.

Разработка прототипа. В разрабатываемом прототипе предлагается использовать нейронную сеть, обучение которой будет проходить с учителем. Нейросеть будет обучаться на двух изображениях, где результатом сравнения будет true или false (человек на фотографиях один и тот же человек или нет).

Учитель создает набор данных, в котором должно находиться не менее двух фотографий одного человека из многих других.

Причины выбора данного подхода:

- нейросеть переобучаема;
- нейросеть можно «дообучить», добавив новые наборы данных;
- обученная нейросеть даёт быстрые ответы (в рамках решаемой задачи «похож/не похож»);
- всегда можно повысить или убавить порог сходства.

Предлагается следующая структура прототипа СКУД с технологией распознавания лиц:

- Arduino Mega для управления считывателями RFID и турникетами;
- считыватели RFID;
- IP камеры для захвата изображений;
- компьютер с установленным приложением СКУД;
- сервер с базой данных.

Arduino Mega. Электронные устройства Arduino давно зарекомендовали себя на рынке программируемой электротехники как качественный, многофункциональный и недорогой продукт. Поэтому в данном проекте будет использоваться данное электронное устройство модели Mega, которая в свою очередь имеет в своём арсенале 256 КБ флэш-памяти и 8 КБ оперативной памяти.

Считыватель RFID. Данные считыватели нужны для чтения UID (User identifier) со смарт-карт.

IP камера. Для более качественной работы системы понадобятся IP камеры с определёнными характеристиками:

1. Наличие WDR (Wide Dynamic Range) – этот параметр, который влияет на освещённость.
2. Количество кадров в секунду – чем больше кадров в секунду будет снимать камера, тем выше вероятность что камера сделает нужный снимок. В данной задаче потребуется минимум 20 кадров в секунду.
3. Разрешение камеры видеонаблюдения – при большем разрешении будет выше детализация. Высокое разрешение положительно скажется на процессе выявления нейросетью маркеров на полученном снимке.
4. Вариофокальный объектив – объектив, где есть возможность изменить фокусное расстояние.

Компьютер. Минимальные требования для нормальной работы приложения СКУД:

- процессор 2 ядра, частота 1,1 ГГц;
- Windows 7 и новее;
- ОЗУ 2 Гб;
- установленный .NET Framework 4.8;
- 150 МБ свободного места.

Сервер с БД. На сервере должна быть установлена SQL Server Management Studio от компании Microsoft.

Концептуальная модель работы СКУД представлена на рисунке 6.

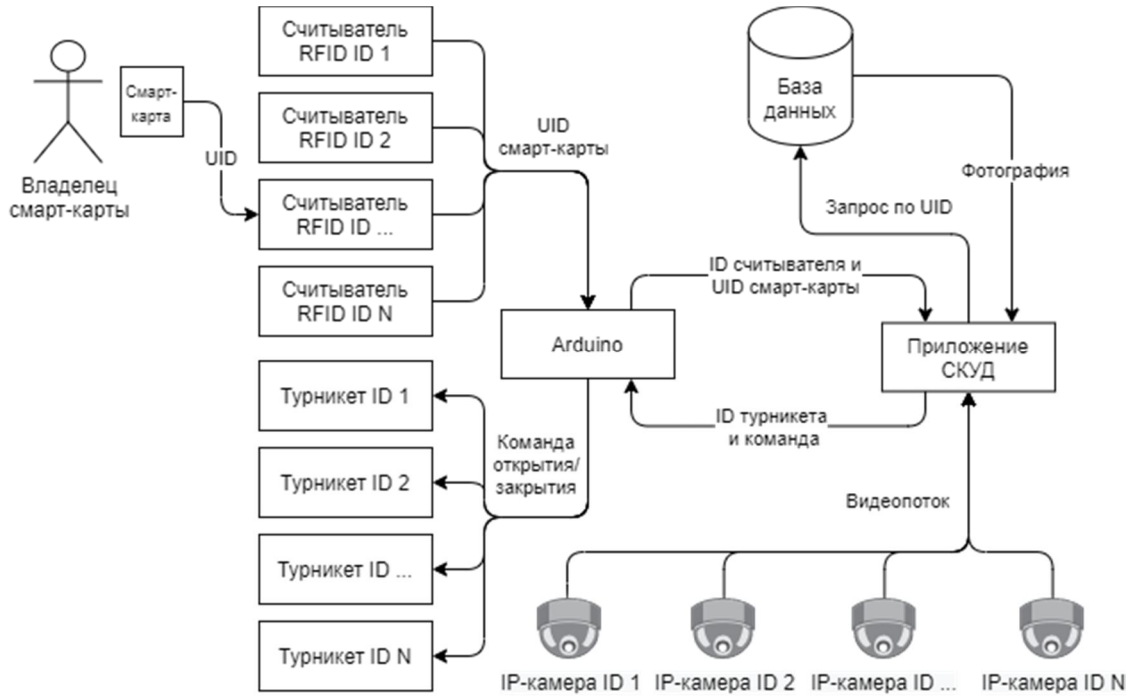


Рисунок 6 – Концептуальная схема работы СКУД

Сценарий использования СКУД с технологией распознавания лиц. Владелец смарт-карты должен поднести смарт-карту к считывателю. Считыватель получает UID поднесённой карты и отправляет его (UID смарт-карты) электронному устройству Arduino. Arduino в свою очередь отправляет на компьютер (с установленным приложением СКУД) по COM-порту UID считанной смарт-карты и ID считывателя, с которого был получен UID. На компьютере приложение СКУД отправляет запрос к базе данных с целью проверки наличия данной смарт-карты в базе, если UID смарт-карты не существует, то перед нами злоумышленник. При обнаружении карты из базы данных выгружается изображение, привязанное к UID считанной смарт-карты. Приложение СКУД проводит анализ на совпадение изображения лица, полученного из базы данных с изображением, полученным с IP-камеры. Если вероятность совпадения ниже некоторого заданного порога, значит, что перед нами злоумышленник и система запретит ему доступ. Если вероятность совпадения изображений выше порогового значения, приложение СКУД отправит на электронное устройство Arduino ID турникета и команду «открыть», а Arduino в свою очередь передаст нужному турникету команду «Открыть».

Блок-схема предложенного решения представлена на рисунке 7.

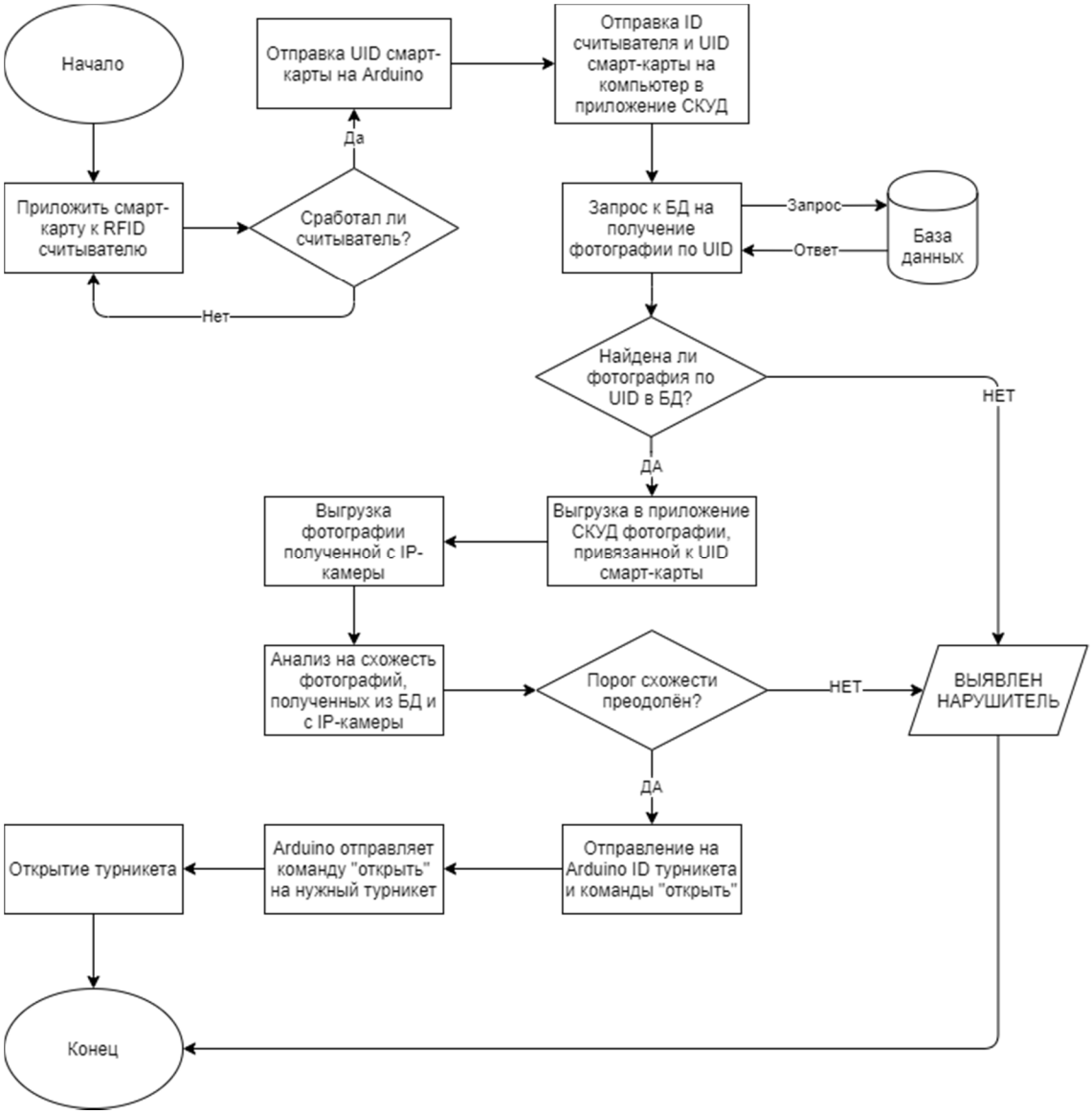


Рисунок 7 – Блок-схема процесса

Заключение.

1. Технологии распознавания лиц планомерно внедряются во многие технологические процессы, в том числе и в системы обеспечения безопасности. СКУД с использованием технологии распознавания лиц способствует детектированию ситуаций, когда для прохода злоумышленник применяет карту легального пользователя путем сравнения лица владельца карты из базы данных организации с изображением лица, пытающегося проникнуть на охраняемую территорию.
2. В работе предложена общая схема процесса контроля и управления доступом с использованием технологии распознавания лиц и продемонстрирована концептуальная схема предложенного аппаратного решения.
3. Усовершенствование СКУД позволит повысить уровень информационной безопасности предприятий и, как следствие, снизить возможный финансовый ущерб от реализации атак на их активы.
4. Бесконтактная идентификация пользователей путем распознавания их лиц актуальна в условиях неблагоприятной эпидемиологической обстановки.

Потенциальными пользователями данной системы могут являться как государственные, так и коммерческие организации, заинтересованные в обеспечении режима конфиденциальности на собственной территории.

Библиографический список

1. Ворожейкин М. Р. Общие сведения о системе распознавания лиц / М. Р. Ворожейкин, С. В. Чернова // Актуальные вопросы науки. – 2019. – № 47. – С. 35–37.
2. Рудинская Е. А. Разработка алгоритма детектирования лиц с использованием комбинаций каскадов Хаара / Е. А. Рудинская, Р. А. Парингер // Сборник трудов ИТНТ-2019. – 2019. – С. 6–12.
3. RFID метки – ультимативный гид по выбору. – Режим доступа: https://securityrussia.com/blog/rfid-metki.html, свободный. – Заглавие с экрана. – Яз. рус.
4. Сайт новостного сервиса «Киосксофт». – Режим доступа: https://kiosksoft.ru/news/2020/05/28/tochnost-beskontaktnoj-identifikacii-otpechatkov-palcev-poka-ostaetsya-nizkoj-71797, свободный. – Заглавие с экрана. – Яз. рус.
5. Власенко А. В. Обзор инструментов машинного обучения и их применения в области кибербезопасности / А. В. Власенко, П. И. Дзьобан, Р. В. Жук // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 1. – С. 144–155.
6. Сиротин Д. В. Перспективы внедрения мобильной идентификации СКУД в корпоративные IT-системы // Алгоритм безопасности. – 2019. – № 2. –С. 38–39.
7. Марьенков А. Н. Система выявления агрессивного поведения людей на основе анализа видеоматериалов с применением рекуррентной сверточной нейронной сети / А. Н. Марьенков, Е. О. Кузнецова, А. А. Приходько // Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики : материалы XIX Международной научно-практической конференции. – Ростов : Ростовский государственный экономический университет, 2019. – С. 207–210.
8. Дёмин К. С. Методы распознавания движений человека с применением технологий нейронных сетей / К. С. Дёмин, А. Н. Марьенков // Математические методы в технике и технологиях ММТТ. – 2020. – Т. 8. – С. 135–138.

References

1. Vorozheykin M. R., Chernova S. V. Obshchiye svedeniya o sisteme raspoznavaniya lits [General information about the face recognition system]. Aktualnye voprosy nauki [Actual Issues of Science], 2019, no. 47, pp. 35–37.
2. Rudinskaya E. A., Paringer R. A. Razrabotka algoritma detektirovaniya lits s ispolzovaniyem kombinatsiy kaskadov Khaara [Development of a face detection algorithm using combinations of Haar cascades]. *Sbornik trudov ITNT-2019* [Proceedings of ITNT-2019], 2019, pp. 6–12.
3. *RFID metki – ultimativnyy gid po vyboru* [RFID tags – the ultimate guide to choose]. Available at: https://securityrussia.com/blog/rfid-metki.html
4. *Sayt novostnogo servisa "Kiosksoft"* [Site of the news service "Kiosksoft"]. Available at: https://kiosksoft.ru/news/2020/05/28/tochnost-beskontaktnoj-identifikacii-otpechatkov-palcev-poka-ostaetsya-nizkoj-71797
5. Vlasenko A. V., Dzoban P. I., Zhuk R. V. Obzor instrumentov mashinnogo obucheniya i ikh primeneniya v oblasti kiberbezopasnosti [Overview of machine learning tools and their use in the field of cyber security]. *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii* [Caspian Journal: Control and High Technologies], 2020, no. 1, pp. 144–155.
6. Sirotin D. V. Perspektivy vnedreniya mobilnoy identifikatsii SKUD v korporativnye IT-sistemy [Prospects for the introduction of mobile identification of access control systems in corporate IT systems]. *Algoritm bezopasnosti* [Security Algorithm], 2019, no. 2, pp. 38–39.
7. Marenkov A. N., Prikhodko A. A., Kuznetsova E. O. Sistema vyyavleniya agressivnogo povedeniya lyudey na osnove analiza videomaterialov s primeneniem rekurrentnoy svyortochnoy neyronnoy seti [A system for detecting aggressive behavior in people based on analysis of video materials using a recurrent conventional neural network]. *Problemy proyektirovaniya, primeneniya i bezopasnosti informatsionnykh sistem v usloviyakh tsifrovoy ekonomiki* [Problems of design, application and security of information systems in the conditions of the digital economy], 2019, pp. 207–210.
8. Marenkov A. N., Demin K. S. Metody raspoznavaniya dvizheniy cheloveka s primeneniyem tekhnologiy neyronnykh setey [Methods for recognizing human movements using technologies of neural networks]. *Matematicheskiye metody v tekhnike i tekhnologiyakh* [Mathematical methods in engineering and technology – MMTT], 2020, pp. 135–138.