Разработка программного обеспечения для управления системой безопасности зданий

Е.Е. Истратова, А.О. Амельченко

***Аннотация*—В статье приведены результаты разработки программного обеспечения для управления системой безопасности зданий. В ходе исследования был проведен анализ существующих систем, разработан собственный алгоритм обработки видеопотоков, выбраны инструментальные средства и реализовано программное обеспечение для управления системой безопасности зданий, позволяющее в режиме реального времени осуществлять контроль за работой пропускной системы, системы видеонаблюдения и системы противопожарной безопасности. Программное обеспечение разработано на языке программирования C++ с применением фреймворка Qt5, библиотеки алгоритмов компьютерного зрения OpenCV и библиотеки для распознавания лиц NCNN. Отличительной особенностью программного решения является его способность работать на встраиваемых системах с малой вычислительной мощностью с различными протоколами передачи видео и других данных, получаемых с датчиков. Программный продукт может применяться для идентификации и учета людей, работающих на предприятии, обеспечения работы пропускной системы, системы видеонаблюдения, а также для контроля за работой датчиков в интеллектуальной системе управления зданием.**

***Ключевые слова*—сверточные нейронные сети, системы управления безопасностью зданий, программное обеспечение, распознавание лиц, идентификация лиц.**

I. Введение

В последние десятилетия стремительное развитие информационных технологий существенно изменило инженерную, экономическую и социальную сферы человеческого общества. Причем резко возрастает спрос на комплексные системы, обеспечивающие интеллектуальное управление зданием. Подобные системы автоматизации и управления зданиями становятся обычным инструментом для обеспечения их безопасности. Это обусловлено рядом факторов, среди которых можно выделить такие, как: коммерческая потребность в функциональности, обмен информацией, снижение затрат при обслуживании зданий.

При этом под интеллектуальным зданием понимается комплекс информационных инструментов, обеспечивающих управление и контроль за системами электроснабжения, отопления, вентиляции и кондиционирования воздуха, вертикальными транспортными системами и системами безопасности жизнедеятельности. Благодаря этому, подобная архитектура системы управления зданием позволяет в автоматическом режиме обеспечивать в каждом помещении наиболее комфортные условия для персонала по температуре, влажности воздуха и освещенности; получать объективную информацию о работе и состоянии всех систем, своевременно сообщать диспетчерам о необходимости вызова специалистов по сервисному обслуживанию; перераспределять энергоресурсы между системами, обеспечивая их эффективное использование и экономию энергоресурсов; обеспечивать централизованный контроль и управление при нештатных ситуациях [1].

Таким образом, автоматизированная система управления зданием, которую также называют системой автоматизации и диспетчеризации инженерного оборудования, является ядром интеллектуального здания и представляет собой аппаратно-программный комплекс, осуществляющий сбор, хранение и анализ данных от различных систем здания, управление работой этих систем через сетевые контроллеры.

II. Анализ применения систем управления безопасностью зданий

Существует множество исследовательских проектов по умным зданиям, которые проводились по всему миру. Благодаря этому, последние достижения в области разработки решений для умных зданий позволили создать практичные системы видеонаблюдения со встроенными функциями обнаружения объектов и распознавания лиц, которые являются точными и достаточно быстрыми для коммерческого использования. В статье [2] были приведены результаты сравнительного анализа различных подходов к обнаружению объектов и распознаванию лиц для использования в системах видеонаблюдения с точки зрения точности и скорости. Было обнаружено, что Faster R-CNN с Inception ResNet V2 имеет максимальную точностиь при сохранении скорости в условиях работы в реальном времени. С другой стороны, Single Shot Detector (SSD) с MobileNet оперативно и достаточно точно работает с большинством приложений. Что касается технологии распознавания лиц, то FaceNet с многозадачными каскадными сверточными сетями (MTCNN) обеспечивает более высокую точность по сравнению с DeepFace и DeepID2+, и при этом работает быстрее. Также была рассмотрена сквозная система видеонаблюдения, которую можно использовать в качестве встраиваемого модуля для более сложных систем. На обученных моделях были проведены различные эксперименты с подробным объяснением наблюдений.

Применение технологии Интернета вещей для

Истратова Евгения Евгеньевна, Новосибирский государственный технический университет, istratova@mail.ru

Амельченко Артем Олегович, Новосибирский государственный технический университет, artemer981333@gmail.com

строительства интеллектуальных зданий может повысить практичность интеллектуальных систем, оптимизировать распределение ресурсов и расширить возможности управления и обслуживания интеллектуальными зданиями, тем самым улучшив качество жизни людей. На основе обобщения и анализа предыдущих исследовательских работ в статье [3] были изучены состояние развития и будущие задачи технологии Интернета вещей, проанализировано влияние данной технологии на интеллектуальные здания и интеллектуальное производство, а также изложена концепция использования интегрированной системной структуры интеллектуального здания для создания модели интеллектуального производства на основе технологии Интернета вещей. Результаты проверки модели показали, что интеллектуальная производственная модель строительной отрасли может реализовать интеграцию человеческого общества и физической системы и достичь цели управления и контроля в реальном времени персонала, машин, оборудования и инфраструктуры в рамках всей сети. Результаты исследования в данной статье могут служить отправной точкой для дальнейших исследований модели интеллектуального производства в строительной отрасли на основе технологии Интернета вещей.

Несмотря на то, что приложения Интернета вещей стремительно развиваются, вредоносные устройства представляют собой серьезную проблему, угрожающую их безопасности. В статье [4] предложено решение — интеллектуальная система для устройств Интернета вещей на базе использования инфраструктуры граничных и облачных вычислений. Предлагаемая система может быть использована для смягчения последствий вредоносных и неисправных устройств Интернета вещей. Таким образом, предложенный программный продукт может использоваться для повышения эффективности систем на основе технологии Интернета вещей, таких как умные города, и снижения риска вредоносных устройств, особенно в чувствительных системах, таких как военные приложения, которые используют устройства Интернета вещей. Для достижения этой цели в статье предлагается новый метод идентификации для уникальной и глобальной идентификации устройств Интернета вещей, где бы они ни перемещались. Результаты показали, что предложенный подход обеспечивает очень хорошие результаты в обнаружении вредоносных устройств Интернета вещей и вычислении значений, близких к истинным.

Системы автоматизации и управления зданиями становятся обычным явлением в зданиях, что обусловлено коммерческой потребностью в функциональности, обмене информацией, снижении затрат при их эксплуатации. Тем не менее, если угроза, проявляемая в системах автоматизации и управления зданиями, реализуется, воздействие на здание может быть значительным в результате отказа, потери или манипулирования зданием и его услугами, что приведет к потере информации. Результаты исследования [5] показали, что большинство специалистов по информационной безопасности осведомлены о проблемах безопасности систем автоматизации и управления зданиями, хотя им не хватает знаний и опыта для обеспечения необходимой защиты. Например, было обнаружено, что понимание 23 уязвимостей систем автоматизации и управления зданиями одинаково важно с ограниченной дисперсией. Стратегии смягчения последствий были не лучше: респонденты указывали на плохую диагностику угроз. Напротив, специалисты по кибербезопасности и технической безопасности, такие как интеграторы или специалисты по проектированию систем безопасности, продемонстрировали четкое понимание уязвимостей систем автоматизации и управления зданиями и соответствующих стратегий их устранения. Полученные данные подтвердили необходимость повышения осведомленности как специалистов по управлению безопасностью, так и специалистов объектов об уязвимостях систем автоматизации и управления зданиями и стратегиях их устранения.

Эксплуатация интеллектуальных зданий требует учитывать ряд факторов: ресурсосбережение, снижение эксплуатационных расходов, повышение безопасности, обеспечение комфортных условий труда и отдыха [6]. Однако автоматизация управления соответствующими инженерными системами освещения, микроклимата, безопасности, коммуникационными системами и сетями с помощью современных технологий, например, Интернета вещей, порождает проблемы, связанные с хранением и обработкой больших объемов данных, степень использования которых сегодня крайне низкая. В связи с тем, что жизненный цикл здания достаточно велик и превосходит жизненный цикл стандартов, учитывающих требования безопасности, комфорта, энергосбережения и т.п., необходимо учитывать аспекты управления в условиях рационального использования больших данных на этапе информационного моделирования [7].

В статье [8] приведены результаты синтеза гибкой архитектуры информационной системы для управления подсистемами технического обеспечения интеллектуального здания, включающей: уровень клиента, уровень приложения и уровень данных, а также три слоя: слой представления, слой исполнительных устройств и слой аналитики. Для решения проблемы, связанной с увеличением объема обрабатываемой контроллером сообщений реального времени информации, было предложено использовать датчики и исполнительные механизмы с настраиваемым порогом срабатывания, реализующие алгоритмы управления на основе модели дискретных автоматов, в частности, логические схемы алгоритмов. В результате исследования было доказано, что готовое программное обеспечение способно повысить качество принимаемых решений и снизить эксплуатационные расходы здания за счет применения контура управления, использующего интеллектуальный анализ данных.

Помимо секторов коммерческой и жилой

недвижимости, сельскохозяйственное производство в настоящее время также имеет невостребованные информационно-управляющие ресурсы для развития и совершенствования агротехнологических процессов и сервиса агропредприятий путем более широкого использования и интеграции средств видеонаблюдения в единую самоорганизующуюся систему аграрного производства. Для дальнейшего совершенствования агротехнологических процессов, повышения скорости и безошибочности управления наиболее перспективным является разработка систем управления роботизированными агротехнологическими комплексами с использованием мобильных дистанционных систем автоматизированного видеонаблюдения, видеоаналитики, видеоадминистрирования [9].

Интеллектуализация процессов контроля и управления строительными объектами разного типа, начиная от жилых и административных зданий и кончая мостами и дамбами, является в настоящее время одним из наиболее важных и перспективных направлений развития коммунального хозяйства. В связи с этим, анализируются структура и состав контролируемых факторов подсистемы сбора данных в рамках систем интеллектуального управления зданием. В литературном источнике [10] здание рассматривается как социотехническая система, в которой непротиворечиво и бесконфликтно соединены все технические элементы здания и все субъекты, находящиеся в здании на законных основаниях – легитимные субъекты. Предложена общая структура систем интеллектуального управления зданием, в которой выделено шесть отдельных самостоятельных подсистем: подсистема жизнеобеспечения; подсистема безопасности; подсистема информационной поддержки; подсистема сбора данных; подсистема обеспечения комфортности легитимных субъектов; подсистема управления и развития. Применительно к подсистеме сбора данных проведена классификация факторов, влияющих на процесс функционирования интеллектуального здания, и на этой основе описана процедура формирования состава каналов воздействия на систему интеллектуального управления зданием и ее элементы, а также состав данных, которые необходимо собирать для эффективного функционирования итоговой системы.

Внедрение автоматизированных и информационных технологий в области эксплуатации зданий и инженерных систем позволяют повысить эффективность их использования и обеспечить расходование ресурсов. При этом наиболее важным является возможность повышения эффективности использования энергоресурсов, потребляемых в процессе эксплуатации. В статье [11] рассмотрены методы эксплуатации зданий и инженерных систем с применением автоматизированных систем эксплуатации, методы обработки информации об объекте эксплуатации.

Таким образом, на основании анализа литературных источников можно сделать вывод о востребованности создания программного обеспечения для управления системой безопасности зданий, позволяющего в режиме реального времени осуществлять контроль за работой: пропускной системы, а также таких систем, как видеонаблюдение и противопожарная безопасность.

III. Структура системы управления безопасностью зданий

Современные системы управления безопасностью зданий имеют четко организованную структуру (рис. 1), в состав которой входят такие модули, как: система видеонаблюдения; пропускная система; система противопожарной безопасности; система сигнализации; система контроля протечек.

Рис. 1 - Структура системы управления безопасностью здания

В рамках реализации работы были рассмотрены три системы, интегрируемые в один программный продукт при помощи центрального сервера, выступающего в качестве связующего звена системы. К указанным системам относятся следующие: система видеонаблюдения, пропускная система и система противопожарной безопасности.

1. Система противопожарной безопасности. В первую очередь, система безопасности здания должна обеспечивать эффективное обнаружение чрезвычайных ситуаций и оповещение всех людей, находящихся в здании, об их возникновении. Для этого в программном обеспечении должна быть предусмотрена возможность непрерывной обработки данных, поступающих с датчиков, в том числе с датчиков дыма, температуры и других, служащих для обнаружения возгорания. Также для своевременного информирования людей необходимо предусмотреть работу с системой оповещения, установленной в здании. Примеры подобных систем приведены в литературных источниках [12,13].

2. Пропускная система на основе технологии компьютерного зрения. Следующей по важности частью комплексной системы безопасности здания является модуль пропускной системы, который применяется как на входе в здание для распознавания лиц, так и при въезде на территорию для определения государственных номеров автомобильного транспорта. Технология

компьютерного зрения для распознавания лиц позволяет сделать проход через пропускной пункт быстрым и безопасным: человеку достаточно показать лицо в камеру на несколько мгновений и система подаст сигнал для пропуска или для запрета прохода в здание. Подобная тактика позволяет избежать выдачи пропусков сотрудникам, что не является достаточно надежной защитой, поскольку пропуск можно потерять, либо он может быть украден, в этом случае злоумышленник сможет проникнуть на предприятие под видом сотрудника. Система распознавания лиц позволяет избежать подобных случаев. Примеры подобных систем приведены в литературных источниках [14,15]. Однако пропускная система на основе применения технологии компьютерного зрения для распознавания лиц не будет эффективна в случае, если этот процесс будет занимать много времени. Поэтому необходимо подобрать достаточно оперативный и устойчивый к помехам метод.

3. Система видеонаблюдения. Помимо распознавания лиц, система безопасности здания должна быть оснащена системой видеонаблюдения. Для реализации подобных систем чаще всего применяются защищенные системы видеонаблюдения, видеомониторинга и видеоаналитики, отличающиеся функциональным составом и характеристиками [16]. Так, современные системы видеонаблюдения все чаще оснащаются функциями анализа видеоконтента для самых разных приложений. Однако надежность и надежность алгоритмов анализа видеоконтента остаются проблемой. Их необходимо сравнивать с достоверными данными, чтобы количественно оценить производительность и точность новых алгоритмов. В литературе описано множество методов. Пример цифровой системы видеонаблюдения на базе сети приведен в литературном источнике [17]. В статье [18] представлены результаты разработки программной среды для непрерывной оценки и документирования производительности систем видеонаблюдения на основе применения набора репрезентативных показателей в качестве фундаментальной части системы оценки. В литературном источнике [19] сообщается о разработке автоматизированной встроенной системы видеонаблюдения с использованием двух специализированных встроенных RISC-процессоров. Результаты экспериментов подтвердили, что система способна обнаруживать, отслеживать и кодировать изображения с движением объектов в них в режиме реального времени.

Таким образом, предварительный анализ литературных источников позволил сделать выводы об актуальности и востребованности разработки программного обеспечения для управления системой безопасности зданий.

IV. Разработка алгоритма обработки видеопотока

В качестве объекта автоматизации в рамках выполнения работы был рассмотрен программный продукт, цель которого заключалась в автоматизации процессов сбора, обработки и анализа данных, поступающих со следующих трех модулей системы управления безопасностью здания:

1. Модуль пропускного пункта здания.
2. Модуль обработки датчиков системы безопасности здания.
3. Модуль видеонаблюдения здания.

Каждый из трех модулей взаимодействует с центральным сервером, отправляя ему соответствующие данные, собираемые в ходе работы модулей. Помимо этого, предусмотрен режим работы, когда в случае невозможности соединения с сервером каждый модуль может работать автономно, а затем, при подключении к серверу, будет способен синхронизировать передаваемые данные.

В процессе работы первого модуля осуществляется сбор и анализ видеопотоков, содержащих изображения посетителей. При обнаружении лица человека система отображает информацию о нем поверх полученного изображения. В случае, если человека удалось идентифицировать, система принимает решение, пропустить его в здание или нет, а также заносит в базу данных информацию о его посещении. Если система приняла решение пропустить идентифицированного человека, то она посылает сигнал на открытие соответствующего турникета.

В процессе работы второго модуля осуществляется мониторинг различных данных, поступающих с датчиков системы безопасности здания. Система с определенной периодичностью запрашивает данные с каждого датчика, указанного в настройках. Период опроса задается для каждого датчика индивидуально, как и диапазон приемлемых значений и время допустимого отклонения от этого диапазона. В случае, если датчик в течение времени больше допустимого выдавал значения, выходящие за приемлемый диапазон, то система сигнализирует об этом теми способами, которые предварительно задал пользователь.

В процессе работы третьего модуля осуществляется интеграция программного комплекса с системой видеонаблюдения.

Таким образом, цель разрабатываемого программного обеспечения заключается в сборе, обработке и анализе всех типов данных, поступающих с датчиков системы безопасности, системы видеонаблюдения и пропускной системы в режиме реального времени, что в результате позволяет обеспечивать контроль и управление в системе безопасности здания.

Для реализации указанной цели программным обеспечением решаются задачи по сбору, обработке и анализу исходных данных, поступающих в него, а также по визуализации выходных потоков данных.

В качестве информации, подаваемой на вход программного обеспечения, можно перечислить следующие информационные потоки:

1. Информация, поступающая с датчиков системы безопасности (датчики температуры, задымления, возгорания, протечки и т.д.) для

информирования о непредвиденной ситуации в случае обнаружения таковой.
2. Видеопотоки для обнаружения и идентификации людей, информация о которых внесена в базу данных.

К исходящей информации относятся следующие информационные потоки:

1. Информация об обнаруженных и идентифицированных людях.
2. Сигнал об открытии турникета в случае возможности прохода идентифицированного человека.
3. Сигнал о наступлении непредвиденной ситуации в системе безопасности.

Для реализации указанных задач при проектировании программного обеспечения были предусмотрены две основные роли пользователей: администратор и оператор. Основными функциями пользователя с ролью администратор являются: добавление, редактирование, удаление информации о персональных картах, пропускных реле, камерах видеонаблюдения. Пользователь с ролью оператор может просматривать персональные карты, выдавать разовые пропуски гостям и открывать турникет «вручную».

В задачах компьютерного зрения лучшие результаты неизменно показывают алгоритмы машинного обучения, основанные на глубоких нейронных сетях, демонстрируя при этом более точные результаты при решении задач классификации по сравнению с возможностями человека. Чтобы распознать лицо, необходимо произвести определение местоположения объекта заранее заданного класса, определить его координаты. Задачу определения местоположения объекта в кадре можно назвать «детектированием». Существует множество подходов к детектированию лица, каждый из которых отражается в архитектуре нейронной сети. Некоторые архитектуры, такие как, например, Faster R-CNN, включают две нейросети. Одна из них предсказывает регион интереса объектов на изображении, в котором, скорее всего, будет лицо, а другая нейронная сеть является классификатором и определяет, что внутри региона присутствует объект нужного класса. В проведенном исследовании данная архитектура была переработана и улучшена.

Чтобы реализовать алгоритм распознавания лиц, который был бы устойчивым к попыткам злоумышленников воспользоваться несовершенством системы аутентификации и подменить свои биометрические данные, выдав себя за другого человека, были проанализированы все доступные алгоритмы.

В настоящее время существует множество способов обмануть алгоритм распознавания, например, предъявить вместо своего лица распечатанную цветную фотографию или изображение лица другого человека на дисплее мобильного устройства, телефона или планшета. На данный момент область исследования в рамках компьютерного зрения, занимающаяся решением проблем неустойчивости алгоритмов к обману, называется face anti-spoofing. Попытка обмана системы называется spoofing attack, а комплекс защитных мер против такого рода атак, реализованный в алгоритме распознавания, называется anti-spoofing.

Одним из распространенных методов борьбы со spoofing attack является анализ нескольких кадров видеопотока на предмет наличия движений: повороты, моргания, мимика лица. Пользователю может быть предложено совершить случайный набор действий, а затем последовательность действий анализируется, заранее подготовиться к ней злоумышленнику непросто, что увеличивает устойчивость системы. При печати картинки или демонстрации фотографии на дисплее в кадре возможно обнаружить особенности ухудшения качества изображения, локальные паттерны. Таким образом, в общем виде алгоритм сводится к расчету интенсивностей пикселей, затем последовательно берется каждый пиксель изображения и восемь его соседей, после чего сравнивается их интенсивность. По полученным последовательностям строится попиксельная гистограмма, которая подается на вход SVM (support vector machine) - классификатора.

Помимо классических подходов машинного обучения, существует крупная область anti-spoofing подходов, в которой используются нейронные сети. Решение проблемы распознавания лиц может быть решено путем ансамблирования нейросетей или создания сложных архитектур с использованием различных признаков с дополнительными алгоритмами. При этом получаются достаточно убедительные результаты с высокой точностью.

В результате анализа существующих моделей, алгоритмов и методов обработки видеопотоков, а также с учетом цели, задач и функций разрабатываемого программного обеспечения были сформулированы основные требования, предъявляемые к его работоспособности. В качестве основных из них можно выделить следующие:

1. Возможность добавления камер.
2. Возможность добавления реле для открытия турникетов.
3. Возможность обработки видеопотоков, поступающих с камер, для дальнейшего распознавания и идентификации лиц на них.
4. Возможность открытия соответствующего турникета в случае санкционированного прохода сотрудника.
5. Подключение к центральному серверу для синхронизации и отправки всех происходящих событий.
6. Возможность добавления, редактирования и удаления карточек пользователей, при наличии на данное действие соответствующих прав.
7. Возможность получения фотографических изображений сотрудников и клиентов из видеопотока.

Для добавления камер и реле в программном обеспечении должны быть реализованы соответствующие сценарии, вызываемые из интерфейса.

При добавлении камеры должна быть предусмотрена реализация возможности по выбору реле, на которое будет подаваться сигнал при пропуске человека, подошедшего к данной камере. При добавлении реле в обязательном порядке должен быть выведен в пользовательский интерфейс текст запроса на его открытие. Обработка видеопотоков с функциями распознавания и идентификации лиц должна осуществляться для всех добавленных в приложение камер. При этом каждый видеопоток должен обрабатываться в отдельном потоке.

Таким образом, исходя из всех перечисленных особенностей реализации, алгоритм обработки видеопотока должен включать следующие действия:

1. Получение кадра с камеры.
2. Приведение кадра к необходимому разрешению для дальнейшего распознавания нейронной сетью.
3. Распознавание всех лиц в кадре.
4. Выбор из всех распознанных лиц одного, занимающего максимальную площадь кадра.
5. Сопоставление выбранного лица с изображениями, находящимися в базе данных, и определение того, которое обладает наибольшей степенью схожести с распознанным лицом.
6. Идентификация человека. Если степень схожести двух лиц больше или равна установленному порогу, то вывести информацию об идентификации человека. Если степень схожести двух лиц меньше установленного порога, то вывести информацию о невозможности идентификации человека.
7. Вычисление достоверности, то есть подтверждение того, что лицо в кадре является настоящим.

Распознавание лиц в используемой нейронной сети NCNN происходит следующим образом: нейросеть находит координаты глаз, кончика носа и уголков губ, а также координаты прямоугольника, в котором находится лицо. Существует множество нейронных сетей, находящих координаты гораздо большего количества точек лица, что позволяет сильно увеличить точность распознавания. Однако для работы таких нейронных сетей в режиме реального времени необходимы большие вычислительные мощности, что не укладывается в рамки поставленной задачи.

При идентификации лица происходит вычисление углов и расстояний между векторами, соединяющими точки лица, полученные при распознавании. Вычисление происходит с учетом поворота и наклона головы, что позволяет избежать ложных срабатываний. Для того, чтобы считать человека идентифицированным необходима заранее заданная доля совпадения между углами и расстояниями, полученными путем анализа текущего кадра, и теми, что были посчитаны при добавлении сотрудника в базу данных.

После успешной идентификации личности сотрудника необходимо принять решение о том, может ли он пройти. Принятие этого решения регулируется несколькими факторами:

1. Последний зарегистрированный проход сотрудника (вход или выход).
2. Степень достоверности лица.
3. Время, прошедшее с последней идентификации данного сотрудника данной камерой, что необходимо для предотвращения ситуации, когда турникет открывается каждые 300 мс, что составляет период идентификации.

В случае, если сотрудник может пройти, то есть не нарушено зонирование и степень достоверности позволяет считать лицо настоящим, то происходит открытие привязанного к данной камере турникета, а также занесение события в базу данных. Также осуществляется отправка данных о событии на центральный сервер.

Таким образом, на основе всей полученной информации был разработан алгоритм обработки видеопотока, изображенный на рис. 2. Отличительными особенностями полученного алгоритма являются следующие: обнаружение лиц осуществляется через каждые 2 кадра, а идентификация производится каждые 300 мс. Подключение к серверу происходит при запуске программного обеспечения. В случае, если подключиться не удалось, попытки подключения повторяются через заданный период времени. При успешном подключении происходит синхронизация событий, произошедших в период его отсутствия. Далее в процессе работы приложения все происходящие события отправляются на центральный сервер. В случае разрыва соединения события начинают накапливаться в локальном хранилище и ждать подключения.

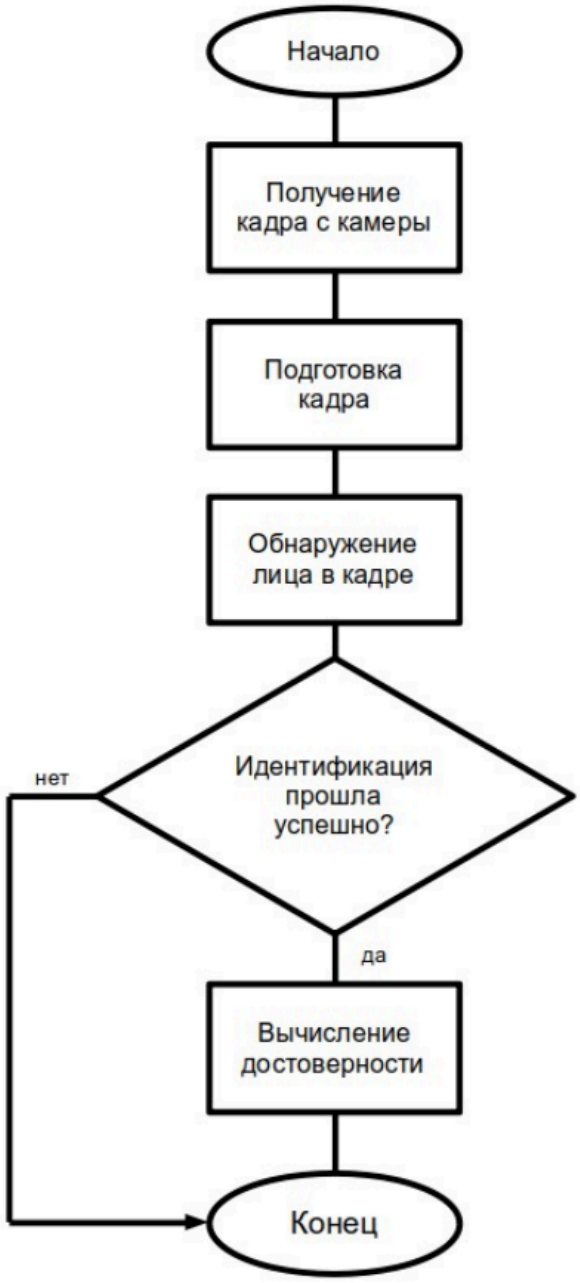

Рис. 2 — Алгоритм обработки видеопотока

Добавление, редактирование и удаление карточек сотрудников происходит при соответствующем запросе из интерфейса. Перед тем, как совершить действие, происходит проверка роли текущего пользователя на возможность выполнять данное действие. Настройку ролей пользователей также производится с помощью программного обеспечения. Роль привязана к пользователю. При открытии программы осуществляется процесс авторизации. Информация о каждом действии, выполняемом с карточками сотрудников, отправляется на центральный сервер и сохраняется в истории. Вместе с информацией о самом действии происходит сохранение записи о том, кто это действие сделал. При добавлении и редактировании карточки сотрудника есть возможность регулировать яркость и контраст изображения, что при правильном использовании позволяет повысить качество идентификации.

V. Разработка программного обеспечения для управления системой безопасности зданий

Алгоритмы машинного обучения, основанные на сверточных нейронных сетях, в настоящее время активно используются во множестве приложений для обнаружения объектов. Тем не менее, многие устройства с ограниченными вычислительными ресурсами и жесткими ограничениями по энергопотреблению не подходят для запуска таких алгоритмов, разработанных для высокопроизводительных компьютеров. Это подтверждает актуальность разработки архитектуры, предназначенной для применения в портативных и ограниченных по мощности ресурсов системах. Отличительными особенностями предлагаемого решения на основе сверточных нейронных сетей является возможность работы в режиме реального времени и с высокой эффективностью.

Система распознавания объектов обычно включает три этапа: предварительную обработку изображения, распознавание изображения и его отслеживание. На каждом этапе требуется выбор оптимального инструментального средства на основе его оценивания для получения наилучшей производительности системы в целом. Каждый из инструментов имеет свои сильные и слабые стороны, которые следует учитывать при выборе оптимальной архитектуры для распознавания объектов. Процедура оценивания была выполнена на основе таких критериев, как: точность, скорость, характер использования оперативной памяти.

Таким образом, выбор инструментальных средств для реализации разрабатываемого программного обеспечения включал в себя следующие этапы: определение необходимых групп инструментов, выбор и обоснование конкретного инструмента в каждой из групп.

В качестве основных групп инструментов были выбраны следующие:

1. Язык программирования.
2. Система управления базами данных.
3. Нейронная сеть для распознавания лиц.
4. Библиотека для обработки изображений.
5. Фреймворк для реализации интерфейса.

Программное обеспечение для управления системой безопасности зданий работает в режиме реального времени, поэтому необходимо выбрать такой язык программирования, который сможет обеспечить высокую производительность. Также необходимо учитывать тот факт, что программное решение является встраиваемой системой и должно работать на одноплатных компьютерах и иметь малое потребление ресурсов. Именно поэтому оптимальным вариантом для реализации программного обеспечения является язык программирования C++, представляющий собой компилируемый, статически типизированный язык программирования, способный обеспечить более высокую производительность по сравнению с другими

высокоуровневыми языками программирования.

Для программного решения необходимо обеспечить создание, подключение и использование базы данных. С учетом требований, предъявляемых к разрабатываемому программному обеспечению, в качестве оптимального решения была выбрана система управления базами данных SQLite, так как она представляет собой программный продукт на основе языка программирования C, который не имеет сервера и позволяет хранить всю базу локально на одном устройстве. Для работы SQLite не нужны сторонние библиотеки или службы. Также стоит учесть, что данная система управления базами данных является наиболее подходящей для использования на встраиваемых системах. Ее основными преимуществами являются следующие: высокая скорость работы; возможность хранения данных в одном файле; легкость администрирования; надежность работы; кроссплатформенность; автономность работы.

В качестве фреймворка для работы был использован NCNN. Это обусловлено тем, что NCNN — это высокопроизводительная вычислительная среда нейронных сетей, оптимизированная для мобильных платформ. Благодаря своим техническим характеристикам и кроссплатформенности, NCNN работает быстрее, чем все известные фреймворки с открытым исходным кодом на процессоре мобильного телефона. Все это позволяет создавать интеллектуальные приложения и использовать искусственный интеллект для задач обнаружения объектов.

В связи с тем, что основное внимание в исследовании уделяется процессу распознавания объектов, а он, в свою очередь, является наиболее ресурсоемкой задачей, то были исследованы современные консолидированные платформы машинного обучения, к которым относятся библиотеки алгоритмов компьютерного зрения. Возможности современных программных библиотек компьютерного зрения обеспечивают решение ряда важных практических задач: анализ содержания изображений, поиск и распознавание заданных объектов, выявление текста, отслеживание движений объектов, выявление общих элементов на сравниваемых изображениях и т. д. При выборе библиотеки алгоритмов компьютерного зрения были изучены следующие библиотеки машинного обучения с открытым исходным кодом: OpenCV, TensorFlow и Qualcomm Neural Processing Software Development Kit (SDK). В результате исследования был сделан вывод о том, что для поставленных целей и задач по обработке изображений и численных алгоритмов общего назначения использование библиотеки OpenCV будет самым оптимальным вариантом.

Для создания интерфейса был использован фреймворк Qt5, представляющий собой инструмент для разработки кроссплатформенного программного обеспечения, реализованный на языке программирования C++, сочетающийся со всеми выбранными до этого инструментальными средствами и обладающий всеми необходимыми характеристиками для работы с нейронной сетью.

Программное решение для управления системой безопасности зданий состоит из двух отдельных модулей. Первый модуль включает центральный сервер, который отвечает за получение и обработку данных, поступающих с различных датчиков безопасности. Также данный модуль служит для синхронизации нескольких устройств, на которых установлен второй модуль – пропускной пункт.

Элемент программного обеспечения, связанный с пропускным пунктом является самостоятельным модулем и работает на отдельном устройстве. Такое решение было принято в виду того, что в здании может находиться несколько пропускных пунктов, а также, что пропускная система должна работать вне зависимости от работоспособности центрального сервера. Данный модуль реализован в виде приложения, позволяющего управлять камерами и турникетами. В нем предусмотрена система распознавания и идентификации лиц, позволяющая людям, информация о которых внесена в базу данных, проходить в здание без использования специальных пропусков.

Центральный сервер реализован в виде консольного приложения с возможностью подключения по сети к приложению для управления всей системой.

Так как модуль пропускного пункта служит для пропуска людей в здание, то периодически необходимо сверять данные о пришедшем человеке с данными, «разрешенными» к допуску на территорию, которые хранятся в базе данных. Система распознает попытки спуфинга и не пропускает человека, пытающегося попасть в здание с помощью фотографии внесенного в базу данных человека. Если все условия соблюдены, то модуль посылает запрос на открытие соответствующего турникета. В случае, когда нужно пропустить человека, не внесенного в базу данных, оператор имеет возможность самостоятельно открыть турникет путем нажатия специальной кнопки.

Для успешного распознавания и идентификации людей был реализован алгоритм обработки видеопотоков. Данный алгоритм выполняется параллельно для нескольких видеопотоков, получаемых с камер, установленных на турникетах.

Алгоритм состоит из следующей последовательности действий:

1. Получение кадра с камеры.
2. Распознавание лиц в кадре.
3. Идентификация лиц.
4. Проверка достоверности лиц.

В целях оптимизации было решено производить распознавание лиц через каждые три кадра, а идентифицировать – через каждые 300 мс.

Для распознавания лиц применяется модель NCNN, определяющая координаты глаз, носа и уголков губ. В процессе идентификации эти параметры сравниваются с данными, находящимися в базе данных. В результате выбирается человек, имеющий наибольшее сходство с предоставленными данными. Проверка достоверности

производится путем оценки таких параметров, как: блики, яркость, контрастность, соответствие освещенности.

После каждой успешной идентификации лица в кадре посылается сигнал модулю обработки событий идентификации, содержащему информацию о человеке. Далее принимается решение об открытии турникета и создании соответствующей записи о проходе.

В случае спуфинга, алгоритм не откроет турникет, если установлен соответствующий параметр. Также, чтобы избежать многократного открытия турникета, производится проверка времени последнего появления данного человека в кадре. Если с этого момента не прошло 5 секунд, то запрос на открытие не будет послан. Однако, если при данной идентификации удалось добиться нужного уровня достоверности (определить, что ранее установленный спуфинг был выявлен ошибочно), то будет послан запрос на открытие. В случае нарушения зонирования человек не будет пропущен. Это достигается просмотром последнего события, связанного с ним. Если событие было входом, то человек сможет выйти и наоборот.

В целях увеличения скорости работы программы и избежания небольших задержек во время распознавания и идентификации обработка каждого видеопотока происходит в отдельном потоке. Также в отдельный поток вынесена функция идентификации, что способствует равномерности воспроизведения видеопотока в пользовательском интерфейсе.

Для распознавания и идентификации в программной реализации применяется класс LiveFaceReco. Функция MTCNNDetection отвечает за распознавание, а Identification – за идентификацию. Для корректной работы с множеством видеопотоков и обеспечением параллельности их обработки, а также для связи с интерфейсом служит класс LFRManager. За обработку событий идентификации отвечает класс CardManager. Его главная функция – HandleIdentificationEvent, следит за ведением списка последних событий. Сетевые взаимодействия обрабатывает класс LFRConnection, который отвечает за обмен всеми данными с сервером.

Для синхронизации нескольких пропускных пунктов, а также для централизованного управления данный функционал был реализован на стороне сервера. При этом основными задачами центрального сервера являются следующие:

1. Обработка подключений пропускных пунктов.
2. Хранение и передача информации о персональных картах, пропускных пунктах и происходящих событиях.
3. Управление пропускными пунктами.
4. Обработка данных с датчиков безопасности.

Для работы с сетью были использованы библиотеки Boost Beast и Boost ASIO. Класс LFRConnection отвечает за обработку сетевого взаимодействия с пропускным пунктом. При подключении пропускного пункта к серверу происходит синхронизация персональных карт, сервер отправляет их актуальный список пропускному пункту. Далее на протяжении всего периода подключения осуществляется обмен информацией: сервер посылает клиенту информацию об изменениях персональных карт и команды для управления, а клиент возвращает серверу информацию о происходящих событиях и изменениях персональных карт, если они произошли.

Для установления соединения и синхронизации между пропускными пунктами служит класс LFRConnectionsManager. При поступлении от клиента данных об изменениях в списке персональных карт, всем существующим подключениям производится рассылка об этом.

Обработка данных с датчиков безопасности происходит посредством класса SensorsManager. Данный класс опрашивает каждый датчик с заданной периодичностью и следит за тем, чтобы возвращаемые значения находились в нужном диапазоне. В случае обнаружения заметных отклонений в показаниях датчиков, посылается сигнал на соответствующее устройство сигнализации или данная информация отображается в интерфейсе пользователя.

VI. Заключение

Таким образом, было разработано программное обеспечение для управления системой безопасности зданий [20]. В ходе реализации программного обеспечения были решены задачи по анализу предметной области и характеристике объекта автоматизации; по разработке алгоритма работы программного обеспечения; по выбору инструментальных средств для реализации программы; по разработке программного обеспечения для управления системой безопасности зданий; по обучению модели нейронной сети.

Программное обеспечение разработано на языке программирования C++ с применением фреймворка Qt5, библиотеки алгоритмов компьютерного зрения OpenCV и библиотеки для распознавания лиц NCNN. Разработанная программа может быть использована в учебных, научных и исследовательских целях, а также для обеспечения бесперебойной работы датчиков в системах безопасности зданий.

Библиография

[1] Кавецкая Е.А. Автоматизированная система управления как современная технология управления информационными и инженерными системами здания / Е.А. Кавецкая, Е.В. Толкачева // Актуальные проблемы авиации и космонавтики. — 2018. — № 14. — С. 836-888.

[2] Xu, J. A deep learning approach to building an intelligent video surveillance system. Multimed Tools Appl 80, 5495–5515 (2021). https://doi.org/10.1007/s11042-020-09964-6.

[3] Kong, L., Ma, B. Intelligent manufacturing model of construction industry based on Internet of Things technology. Int J Adv Manuf Technol 107, 1025–1037 (2020). https://doi.org/10.1007/s00170-019-04369-8.

[4] Yaseen, Q., Jararweh, Y. Building an Intelligent Global IoT Reputation and Malicious Devices Detecting System. J Netw Syst Manage 29, 45 (2021). https://doi.org/10.1007/s10922-021-09611-x.

[5] Brooks, D.J., Coole, M. & Haskell-Dowland, P. Intelligent building systems: security and facility professionals' understanding of system

threats, vulnerabilities and mitigation practice. Secur J 33, 244–265 (2020). https://doi.org/10.1057/s41284-019-00183-9.

[6] Викентьева О.Л. Синтез информационной системы управления подсистемами технического обеспечения интеллектуальных зданий / О.Л. Викентьева, А.И. Дерябин, Л.В. Шестакова // Вестник МГСУ. — 2017. — № 10 (109). — С. 1191-1201.

[7] Гучия С.С. Системы охранного видеонаблюдения на базе ip для обеспечения безопасности здания / С.С. Гучия // T-Comm. — 2009. — № 6. — С. 25-27.

[8] Нгуен С.М. Подсистема управления процессом формирования входных данных в системе интеллектуального управления зданием / С.М. Нгуен, Г.А. Попов, И.Ю. Кучин // Прикаспийский журнал: управление и высокие технологии. — 2015. — № 3 (31). — С. 142-158.

[9] Башилов А.М. Новые возможности цифрового видеонаблюдения при интеграции с биотехническими и информационно-управляющими системами / А.М. Башилов, В.А. Королев, В.Н. Легеза // Вестник НГИЭИ. — 2019. — № 7 (98). — С. 39-49.

[10] Нгуен С.М. Подсистема сбора и подготовки исходных данных в составе систем интеллектуального управления зданием / С.М. Нгуен, Г.А. Попов, Е.И. Сироткина // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. — 2019. — № 3. — С. 20-27.

[11] Колчин В.Н. Применение автоматизированных систем эксплуатации зданий и инженерных систем / В.Н. Колчин // Инновации и инвестиции. — 2020. — № 2. — С. 159-161.

[12] Обухов С.А. Интеграция систем противопожарной безопасности в комплексные системы диспетчеризации зданий и сооружений / С.А. Обухов, В.А. Мусатов, В.И. Фоин // Пожары и ЧС. — 2017. — № 2. — С. 42-45.

[13] Качанов С.А. О возможностях сопряжения систем мониторинга и управления безопасностью и жизнеобеспечением зданий и сооружений с единой дежурно-диспетчерской службой / С.А. Качанов, А.И. Запорожец, В.В. Гинзбург // Технологии гражданской безопасности. — 2004. — № 1. — С. 63-71.

[14] Карышев А.А. Разработка системы контроля доступа сотрудников и автомобилей на территорию предприятия / А.А. Карышев, С.А. Медведева // Известия ТулГУ. Технические науки. — 2018. — № 6. — С. 129-134.

[15] Муса А.Ж. Распознавание лиц для системы безопасности / А.Ж. Муса, А.А. Алдашев // Наука и образование сегодня. — 2020. — № 7 (54). — С. 6-9.

[16] Могилин К.А. Интеллектуальные системы видеонаблюдения в комплексах безопасности / К.А. Могилин, В.А. Селищев // Известия ТулГУ. Технические науки. — 2020. — № 3. — С. 89-94.

[17] Chao, J., Xiang-fang, S., Li-hai, L. et al. Digital video surveillance system based on network. Wuhan Univ. J. Nat. Sci. 5, 456 (2000). https://doi.org/10.1007/BF02850774.

[18] Baumann, A., Boltz, M., Ebling, J. et al. A Review and Comparison of Measures for Automatic Video Surveillance Systems. J Image Video Proc 2008, 824726 (2008). https://doi.org/10.1155/2008/824726.

[19] Wang, G., Salcic, Z. & Biglari-Abhari, M. Customizing Multiprocessor Implementation of an Automated Video Surveillance System. J Embedded Systems 2006, 045758 (2006). https://doi.org/10.1155/ES/2006/45758.

[20] Истратова Е.Е., Бухамер Е.А., Амельченко А.О., Ларионов П.С. Программа для контроля за работой датчиков в интеллектуальной системе управления зданием. Свидетельство о регистрации программы для ЭВМ 2022618625, 13.05.2022. Заявка № 2022618353 от 13.05.2022.

Истратова Евгения Евгеньевна. Новосибирский государственный технический университет, г. Новосибирск, Россия. Кандидат технических наук, доцент кафедры автоматизированных систем управления. Количество печатных работ: 97. Область научных интересов: информационные технологии, информационные системы, системы компьютерного зрения. e-mail: istratova@mail.ru (Ответственная за переписку).

Амельченко Артем Олегович. Новосибирский государственный технический университет, г. Новосибирск, Россия. Студент факультета автоматики и вычислительной техники. Количество печатных работ: 4. Область научных интересов: системы компьютерного зрения, искусственный интеллект, информационные технологии.

Development of software for building safety management

E.E. Istratova, A.O. Amelchenko

***Abstract*—The article presents the results of the development of software for managing the building security system. During the study, an analysis of existing systems was carried out, an own algorithm for processing video streams was developed, tools were selected and software was implemented for managing the building security system, which allows real-time monitoring of the operation of the access system, video surveillance system and fire safety system. The software was developed in the C++ programming language using the Qt5 framework, the OpenCV computer vision algorithm library, and the NCNN face recognition library. A distinctive feature of the software solution is its ability to work on embedded systems with low computing power with various protocols for transmitting video and other data received from sensors. The software product can be used to identify and account for people working in the enterprise, ensure the operation of the access system, video surveillance system, as well as to control the operation of sensors in an intelligent building management system.**

***Keywords*—convolutional neural networks, building safety management systems, software, face recognition, face identification.**

REFERENCES

[1] Kavetskaya E.A. Automated control system as a modern technology for managing information and engineering systems of a building / E.A. Kavetskaya, E.V. Tolkachev // Actual problems of aviation and cosmonautics. - 2018. - No. 14. - S. 836-888.

[2] Xu, J. A deep learning approach to building an intelligent video surveillance system. Multimed Tools Appl 80, 5495–5515 (2021). https://doi.org/10.1007/s11042-020-09964-6.

[3] Kong, L., Ma, B. Intelligent manufacturing model of construction industry based on Internet of Things technology. Int J Adv Manuf Technol 107, 1025–1037 (2020). https://doi.org/10.1007/s00170-019-04369-8.

[4] Yaseen, Q., Jararweh, Y. Building an Intelligent Global IoT Reputation and Malicious Devices Detecting System. J Netw Syst Manage 29, 45 (2021). https://doi.org/10.1007/s10922-021-09611-x.

[5] Brooks, D.J., Coole, M. & Haskell-Dowland, P. Intelligent building systems: security and facility professionals' understanding of system threats, vulnerabilities and mitigation practice. Secur J 33, 244–265 (2020). https://doi.org/10.1057/s41284-019-00183-9.

[6] Vikentieva O.L. Synthesis of information management system for technical support subsystems of intellectual buildings / O.L. Vikentieva, A.I. Deryabin, L.V. Shestakova // Vestnik MGSU. - 2017. - No. 10 (109). - S. 1191-1201.

[7] Guchia S.S. IP-based security video surveillance systems for building security / S.S. Guchia // T-Comm. - 2009. - No. 6. - S. 25-27.

[8] Nguyen S.M. Subsystem for managing the process of generating input data in the system of intelligent building management / S.M. Nguyen, G.A. Popov, I.Yu. Kuchin // Caspian Journal: Management and High Technologies. - 2015. - No. 3 (31). — S. 142-158.

[9] Bashilov A.M. New possibilities of digital video surveillance when integrating with biotechnical and information-control systems / A.M. Bashilov, V.A. Korolev, V.N. Legeza // Vestnik NGIEI. - 2019. - No. 7 (98). - S. 39-49.

[10] Nguyen S.M. Subsystem for collecting and preparing initial data as part of intelligent building management systems / S.M. Nguyen, G.A. Popov, E.I. Sirotkina // Vestnik ASTU. Series: Management, Computer Engineering and Informatics. - 2019. - No. 3. - S. 20-27.

[11] Kolchin V.N. Application of automated systems for the operation of buildings and engineering systems / V.N. Kolchin // Innovations and investments. - 2020. - No. 2. - S. 159-161.

[12] Obukhov S.A. Integration of fire safety systems into complex dispatching systems for buildings and structures / S.A. Obukhov, V.A. Musatov, V.I. Foin // Fires and emergencies. - 2017. - No. 2. - S. 42-45.

[13] Kachanov S.A. On the possibilities of interfacing systems for monitoring and managing the safety and life support of buildings and structures with a single duty dispatch service / S.A. Kachanov, A.I. Zaporozhets, V.V. Ginzburg // Civil Security Technologies. - 2004. - No. 1. - S. 63-71.

[14] Karyshev A.A. Development of an access control system for employees and vehicles on the territory of the enterprise / A.A. Karyshev, S.A. Medvedev // News of TulGU. Technical science. - 2018. - No. 6. - S. 129-134.

[15] Musa A.Zh. Face recognition for the security system / A.Zh. Musa, A.A. Aldashev // Science and education today. - 2020. - No. 7 (54). - S. 6-9.

[16] Mogilin K.A. Intelligent video surveillance systems in security complexes / K.A. Mogilin, V.A. Selishchev // News of TulGU. Technical science. - 2020. - No. 3. - S. 89-94.

[17] Chao, J., Xiang-fang, S., Li-hai, L. et al. Digital video surveillance system based on network. Wuhan Univ. J. Nat. sci. 5, 456 (2000). https://doi.org/10.1007/BF02850774.

[18] Baumann, A., Boltz, M., Ebling, J. et al. A Review and Comparison of Measures for Automatic Video Surveillance Systems. J Image Video Proc 2008, 824726 (2008). https://doi.org/10.1155/2008/824726.

[19] Wang, G., Salcic, Z. & Biglari-Abhari, M. Customizing Multiprocessor Implementation of an Automated Video Surveillance System. J Embedded Systems 2006, 045758 (2006). https://doi.org/10.1155/ES/2006/45758.

[20] Istratova E.E., Bukhamer E.A., Amelchenko A.O., Larionov P.S. A program for monitoring the operation of sensors in an intelligent building management system. Certificate of registration of the computer program 2022618625, 05/13/2022. Application No. 2022618353 dated 05/13/2022.