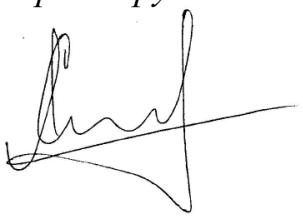
МИНИСТЕРСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И
ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ

Академия Государственной противопожарной службы

На правах рукописи



СОРОКИН ЛЕОНИД АНДРЕЕВИЧ

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ ПОДДЕРЖКА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ В МЕСТАХ МАССОВОГО ПРЕБЫВАНИЯ ЛЮДЕЙ

Специальность 05.13.10 – Управление в социальных и экономических системах
(технические науки)

ДИССЕРТАЦИЯ

на соискание ученой степени
кандидата технических наук

Научный руководитель –
доктор технических наук, доцент,
заслуженный работник высшей школы РФ
Бутузов Станислав Юрьевич

Москва – 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Неотъемлемой составляющей национальной безопасности является общественная безопасность, которая во многом определяет как внутреннюю социально-экономическую стабильность страны, так и статус государства на международной арене. Одним из критериев оценки общественной безопасности является уровень защищенности людей от внутренних угроз, а также последствий стихийных бедствий и техногенных катастроф в местах их массового пребывания. Отметим, что на сегодняшний день особую опасность представляют террористические проявления, которые наряду с угрозой для жизни людей и материальных ценностей подрывают территориальную целостность, суверенитет и конституционный строй Российской Федерации.

В результате анализа статистических данных выявлено, что в России активно увеличивается количество мест массового пребывания людей, так с 2012 г. ежегодно возводится в среднем 13 797 объектов общественного назначения. Однако в то же время, по данным прокураторы Российской Федерации, количество зарегистрированных террористических преступлений в 2016 г. по сравнению с 2012 г. увеличилось более чем в 3 раза, при этом согласно отчетам ФГПУ ВНИИПО МЧС России и Института экономики и мира (Institute for Economics and Peace) экономический ущерб от одного пожара на объектах общественного назначения в среднем составляет 619, 6 тыс. руб., а от одного теракта – 237, 6 млн руб.

Таким образом, с одной стороны в России активно развивается социально-культурная сфера, а с другой стороны, не смотря на активное развитие систем безопасности, нельзя говорить о том, что люди чувствуют себя защищенными, в частности от террористических угроз в местах массового пребывания. Кроме того, современный мир столкнулся с террористическими угрозами нового типа, для реализации которых используются повседневные устройства техногенного

характера. Свидетельством тому служат теракты в Ницце, Берлине, Лондоне, Стокгольме.

Повышение уровня защищённости людей в местах их массового пребывания возможно путем поддержки управления безопасности с использованием современных методов и подходов на основе информационных технологий. Дальнейший анализ выявил целесообразность использования технологий идентификации нарушителя и событий деструктивного характера по изображению.

На сегодняшний день существует множество средств идентификации по изображению. Однако в большинстве случаев они направлены только на информирование об обнаруженном нарушителе, применение же данных технологий для поддержки управления безопасностью людей с учетом особенностей мест их массового пребывания требует новых решений.

Таким образом, актуальность исследования обуславливает необходимость формирования модели и разработки системы информационно-аналитической поддержки управления безопасностью на основе идентификации по изображению с учетом человеческого фактора и особенностей мест массового пребывания людей.

Степень разработанности темы исследования. Решением задач управления безопасностью занималось значительное количество ученых. Существенных результатов в данной области достигли Брушлинский Н.Н., Минаев В.А., Новиков Д.А., Пранов Б.М., Таранцев А.А., Тропченко А.Ю., Топольский Н. Г., Членов А.Н., Cho H., Moon S., Jain L., Jung B., Pan J., Roberts R. и ряд других ученых. Вместе с тем, управление безопасностью людей в местах их массового пребывания имеет ряд особенностей, требующих дополнительного исследования.

Объект исследования – управление безопасностью в местах массового пребывания людей.

Предмет исследования – модели и алгоритмы информационно-аналитической поддержки управления безопасностью в местах массового пребывания людей.

Цель исследования – совершенствование управления безопасностью в местах массового пребывания людей за счет предложенной модели и разработанного алгоритма информационно-аналитической поддержки.

Границы исследования. В диссертационной работе исследуются особенности управления безопасностью в оборудованных автоматизированной системой идентификации по изображению местах массового пребывания людей при несанкционированном проникновении нарушителей.

Научно-техническая гипотеза предполагает возможность повышения защищенности людей в местах их массового пребывания за счет комплексного моделирования процессов управления безопасностью.

Задачи исследования, обеспечивающие достижение цели диссертации:

– анализ управления безопасностью в местах массового пребывания людей;

– формирование модели поддержки управления безопасностью в местах массового пребывания людей, учитывающей особенности реагирования сотрудников, поведения нарушителей и функционирования автоматизированной системы идентификации по изображению;

– разработка системы информационно-аналитической поддержки управления безопасностью людей в местах их массового пребывания на основе идентификации по изображению;

– оценка эффекта от внедрения разработанной системы.

На защиту выносятся:

1. Модель поддержки управления безопасностью в местах массового пребывания людей с комплексным учетом особенностей реагирования сотрудников, поведения нарушителей и функционирования автоматизированной системы идентификации по изображению.

2. Алгоритм поддержки управления безопасностью в оборудованных автоматизированной системой идентификации по изображению местах массового пребывания людей при мониторинге нарушителей и противодействии им.

3. Структура системы информационно-аналитической поддержки управления безопасностью в местах массового пребывания людей на основе идентификации по изображению.

Научная новизна:

1. Предложенная модель, в отличие от существующих, позволяет описать управление безопасностью в местах массового пребывания людей с учетом индивидуальных особенностей сотрудников службы безопасности, поведения нарушителей и параметров автоматизированной системы идентификации по изображению.

2. Особенностью предложенного алгоритма поддержки управления является возможность обоснованного расчета числа и мест дислокаций сотрудников службы безопасности на основе оценки вероятности обнаружения нарушителей и прогнозирования их маршрутов следования с учетом особенностей мест массового пребывания людей.

3. В алгоритме функционирования предложенной системы поддержки управления успешно используются впервые полученные теоретические зависимости скорости реакции от объема информации в базах данных и нагрузки сети видеоконтроля, а также усовершенствованный гибридный метод идентификации на основе уникальности биометрии лица.

Теоретическая значимость обусловлена тем, что полученные модели и алгоритмы информационно-аналитической поддержки развивают теоретико-методологическую базу принятия решений при управлении безопасностью в местах массового пребывания людей.

Практическая значимость определяется возможностью использования полученных результатов для повышения безопасности людей в местах их массового пребывания, что подтверждается разработанным и зарегистрированным

в Роспатенте программным обеспечением системы информационно-аналитической поддержки, которое позволяет повысить результативность и снизить время принятия решений при управлении безопасностью.

Методы исследования. Исследование базируются на методах системного анализа, теории управления, математической статистики, теории графов, теории распознавания образов, теории вероятностей, кластерного анализа.

Достоверность полученных результатов обеспечивается использованием методов исследования, соответствующих задачам, корректным применением апробированного математического аппарата, что подтверждается согласованностью полученных результатов с работами других исследователей и применением материалов диссертации:

– при управлении мероприятиями по противодействию общественно-опасным преступным проявлениям и обеспечению общественного порядка в Олимпийском комплексе «Лужники»;

– в ООО «ИнТех» при разработке, производстве и опытных испытаниях автоматизированных систем поддержки управления безопасностью людей в местах их массового пребывания;

– в учебном процессе Академии Государственной противопожарной службы МЧС России при подготовке бакалавров, специалистов и магистров,

а также наличием свидетельства о государственной регистрации программы для ЭВМ №2016663708 от 14.12.2016 г.

Апробация работы. Основные результаты исследований докладывались и обсуждались на следующих конференциях: Международной научно-технической конференции «Системы безопасности» (Россия, Москва, Академия ГПС МЧС России, 2013 г., 2015 г.), Всероссийской научно-практической конференции с международным участием «Проблемы обеспечения безопасности при ликвидации последствий чрезвычайных ситуаций» (Россия, Воронеж, Воронежский институт ГПС МЧС России, 2015 г.), Международной научно-практической конференции

молодых ученых и специалистов «Проблемы техносферной безопасности» (Россия, Москва, Академия ГПС МЧС России, 2016 г., 2017 г.).

Публикации. Основные научные результаты отражены в 12 публикациях, из них 5 опубликованы в журналах, включенных в перечень ВАК России, в том числе 9 работ изданы в единоличном авторстве.

Личный вклад автора. В опубликованных работах автором изложены результаты, связанные с разработкой модели, алгоритма и системы поддержки управления безопасностью людей в местах их массового пребывания на базе идентификации по изображению, теоретическими обобщениями и прикладными расчетами.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения, четырех приложений, перечня сокращений, списка литературы из 137 наименований. Общий объем диссертации составляет 182 страницы машинописного текста, включая 42 рисунка и 23 таблицы.

ГЛАВА 1. АНАЛИЗ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ЛЮДЕЙ В МЕСТАХ ИХ МАССОВОГО ПРЕБЫВАНИЯ

1.1 Места массового пребывания людей и их безопасность

Возрастание террористической угрозы во всем мире привело к необходимости проведения оперативных мероприятий на совершенно новом уровне, что подтверждено требованиями к антитеррористической защищенности мест массового пребывания людей [54].

Так, согласно постановлению Правительства РФ №272 [54], местом массового пребывания людей является объект, на котором при определенных условиях может одновременно находиться более 50 человек. В рассматриваемом постановлении указывается, что повышение защищенности данных объектов можно достигнуть за счет контроля обстановки «в едином информационном пространстве в режиме реального времени» и «применения современных информационно-коммуникационных технологий». Кроме того, все места массового пребывания людей в обязательном порядке должны оборудоваться системой видеонаблюдения. Также в данном постановлении определяется, что защищенность должна «обеспечивать наиболее эффективное и экономное использование сил и средств, задействованных в обеспечении безопасности мест массового пребывания людей».

Таким образом, защищенность мест массового пребывания людей при эффективном и экономном использовании сил и средств может быть повышена за счет использования информационно-аналитической системы (далее – ИАС) поддержки управления безопасностью на основе компьютерного зрения, которая может использоваться для координации сил и средств охраны при проведении мероприятий прогнозирования, обнаружения и противодействия дестабилизирующим проявлениям интересантов. Кроме того, данная система

способна оповещать о разыскиваемых лицах на объекте, пожаре, появлении дыма и т.д.

Более того современный мир столкнулся с террористическими актами принципиально нового характера. Для совершения теракта уже не нужно оружие или взрывчатое вещество. Свидетельством тому служит теракт в г. Ницце во время празднования Дня взятия Бастилии. Выходец из Туниса на грузовом автотранспорте задавил множество людей на набережной. По свидетельствам очевидцев автомобиль делал зигзаги и намеренно совершал наезды на пешеходов. Погибло 84 человека [64]. «Власть бессильна перед новыми террористическими угрозами. Радикалы действуют непредсказуемо» — таков итог крайне эмоционального совещания кабмина в Париже [86].

Одним из инструментов борьбы с подобными террористическими актами, где в качестве оружия террористы используют устройства техногенного характера, может выступать предлагаемая система. С ее использованием возможно отследить и проанализировать траекторию движения автомобиля или квадрокоптера. Нейтрализация техногенного устройства представляется возможным с использованием высокомощного импульсного генератора электромагнитного излучения [107]. Адаптация данного устройства и сопряжение с системой отслеживания траектории движения представляется возможным в рамках отдельной научно-исследовательской работы.

Технологии на основе распознавания лиц довольно широко используются правоохранительными и государственными органами в зарубежных странах. Известно об успешном их применении военной разведкой США в Афганистане при отслеживании перемещения террористов, полицией Нью-Йорка, Чикаго, Сан-Диего для поиска преступников [118]. В сентябре 2015 года правительство Австралии инвестировало $18,5 млн в программу The National Facial Biometric Matching Capability масштабного повсеместного видеонаблюдения и распознавания лиц. В рамках этой программы предполагается наличие базы данных на 100 млн лиц, собранной со всей Австралии [117].

Такие системы устанавливаются в аэропортах, на улицах городов, в местах большого скопления людей. Однако до сих пор повышение уровня безопасности происходит в основном за счет, увеличения количества проверяющих людей при входе в метро, вокзалы, аэропорты и т.д. По причине того, что человеческий поток в таких местах огромен, данный подход нельзя назвать эффективным.

Существующие системы не ориентированы на быстрый поиск по фотографии в базе данных изображений лиц. Обычно поиск по фотографии в них осуществляется полным перебором изображений все лиц в базе данных. Численность населения Москвы на 1 января 2015 года по оценке федеральной службы государственной статистики составляет 12 108 257 [12]. Глава метрополитена Дмитрий Пегов на выступлении в Совете Федерации, заявил что ежедневный поток пассажиров московского метро составляет 8 000 000 человек [12].

При этом в московском метро на данный момент установлено 5 500 камер и еще планируется установить 22 000 камеры ([6], [43]). Правительство РФ также планирует расходы денежных средств на видеонаблюдение. Согласно [69] на «обеспечение видеонаблюдения, автоматического обнаружения и распознавания целей и тревожных ситуаций в режиме реального времени по видеоизображению и формирование в режиме реального времени базы данных распознанных целей» было выделено в 2011 году – 151 млн. рублей, а 2012 году – 157 млн. рублей». Такие большие суммы позволяют говорить об установке множества видеокамер для видеоанализа.

Все указанные системы содержат в своем составе как серверную, так и клиентскую части. Клиентская часть обычно включает в себя программы видео-фиксации, иногда регистрации заданных событий, а также передачи их на сервер в виде видеопотока иногда с определёнными отметками в некоторых группах кадров. Серверная часть служит для сбора и накопления данных, поступающих с различных видеокамер, сортировки видеоматериалов и их последующего хранения. Объем собранной информации по такому городу, как Москва, составляет до 10 экзабайт (2^{60} байт = 2^{20} терабайт) информации в сутки [25]. Даже

для хранения такого количества информации требуются огромные вычислительные ресурсы, не говоря уже об анализе ее оператором. Как правило, такой анализ выполняется в ходе простого отсматривания видео-материала специалистами, количество которых может отличаться от количества видеокамер где в сотни, а где и в десятки тысяч раз. Поэтому выявить в данном видеопотоке лица, разыскиваемые за неправомерные деяния, или проанализировать поведение людей в реальном времени вряд ли возможно даже при увеличении числа проверяющих в десятки раз без применения автоматизации.

Использование систем видеонаблюдения в сфере безопасности, как правило, не предназначено для массовой биометрической идентификации, анализа поведения и маршрута перемещения человека. Фактическое их назначение – оказание помощи сотрудникам подразделений безопасности в их основной работе. Решения по оценке деятельности интересантов принимает сотрудник подразделения безопасности после выполнения ряда процедур в соответствии с регламентом. Задачи перемещения акцента деятельности по ряду основных функций служб безопасности в виртуальный мир – в область автоматизированного распознавания лиц интересантов, анализа их прошлого, текущего поведения и выдачи рекомендаций по принятию ими решений – перед системами видеонаблюдения ставились достаточно редко. Как правило, в таких случаях решались конкретные отдельные задачи, решаемые в ходе оперативных мероприятий.

Тем не менее, объём собираемой и обрабатываемой информации в ИАС требует автоматизации функций распознавания объектов и принятия решения по ним. Однако в применяемых ныне ИАС, особенно в рамках проведения мероприятий, где имеет место массовое пребывание людей, применение систем с распознаванием рекомендуют проводить только при входах в какие-то ограниченные пространства. Технология и инструкции предписывают службам безопасности создавать условия для наилучшего распознавания путём фиксации интересантов напротив видеокамер в требуемом ракурсе. Однако, учитывая ограничения в оборудовании и допущения алгоритмов распознавания, реальный

процесс выявления потенциально опасных людей предполагает, что часть из них всё-таки не будет распознана. Эта ошибка таких систем первого рода, ее часто называют FRR (False Rejection Rate) [78].

Результатом будет возможное преступное деяние, зафиксированное в местах массового пребывания людей, но не распознанное оператором службы безопасности. Поэтому создание таких систем безопасности, в которых возможно максимально автоматизировать распознавание интересантов по множеству биометрических особенностей в реальном времени и составить для служб безопасности списки потенциально опасных посетителей мероприятий, учитывая террористическую угрозу, крайне актуально в настоящее время ([33], [30]).

Рассмотрим реализацию идентификации в реальных системах.

1.2 Анализ систем поддержки управления безопасности на основе идентификации по изображению

Системы биометрической идентификации на основе уникальности биометрии человека начали применяться в конце прошлого века. Так «в ноябре 1998 года городской комитет Ньюхема принял решение развернуть на своих улицах комплексную систему видеонаблюдения, состоящую из 206 камер, интегрированных в систему автоматического распознавания.

Система замкнутого видеонаблюдения контролирует наиболее важные районы города, поступающий видеосигнал немедленно и автоматически обрабатывается программой, которая осуществляет поиск в базе данных лиц известных полиции преступников и подозреваемых. При совпадении система оповещает оператора, предлагает провести проверку идентичности человека и определить, стоит ли полиции уделять дальше ему внимание или нет. Если совпадения не происходит, то лицевые изображения, отсканированные системой для сопоставления, удаляются из памяти. Результаты работы программы поистине впечатляют: уровень нападения на граждан снизился на 21%, нанесение ущерба имуществу граждан сократилось на 26%, а уровень краж имел беспрецедентное

снижение на целых 39%.» [78].

Биологические объекты (люди и их отдельные характеристики: глаза, температура тела, поведение, походка, особенности движения) обладают рядом уникальных физиологических особенностей, которые сложно изменить или подделать. «Тенденция значительного улучшения характеристик биометрических идентификаторов и снижения их стоимости приведет к широкому применению биометрических идентификаторов в различных системах контроля и управления доступом. В настоящее время структура этого рынка представляется следующим образом: верификация голоса – 11 %, распознавание лица – 15 %, сканирование радужной оболочки глаза – 34 %, сканирование отпечатков пальцев – 34 %, геометрия руки – 25 %, верификация подписи – 3 %.» ([11], с.57).

В связи с тем, что видеокамеры не фиксируют геометрию руки, почерк человека и его отпечатки пальцев, будем рассматривать в качестве базовых характеристик, применяемых в автоматизированных системах идентификации в местах массового пребывания людей, только геометрию лица. А также возможно и характеристики, основанные на походке и особенностях индивидуального трекинга (особенностей движения в конкретных условиях). Кроме того, будем рассматривать автоматизированные системы идентификации по изображению способные детектировать деструктивные события, например пожар.

В ходе исследования выполнен анализ функциональных возможностей наиболее распространенных продуктов в области поддержки управления при обеспечении безопасности с использованием средств идентификации по фотопортрету. Результаты анализа представлены в таблице 1.1 и на рисунке 1.1, где H_1 – допустимая стоимость; H_2 – допустимые временные затраты (время идентификации меньше 0,3 с.); H_3 – приемлемая точность результатов (процент идентификации выше 97%), основанная на вероятностях ошибок первого и второго рода (FRR и FAR); H_4 – устойчивость к неконтролируемым условиям; H_5 – способность функционировать в местах массового скопления людей; H_6

– способность аналитической обработка данных, H_7 – способность функционировать в условиях неопределенности.

Таблица 1.1 – Функциональные возможности автоматизированных средств идентификации

№	Наименование	Характеристики						
		H_1	**H_2**	**H_3**	**H_4**	**H_5**	**H_6**	**H_7**
1.	NEC’s Face Recognition (NEC)	нет инф.	–	–	–	–	–	–
2.	Re:Action (VisionLab)	нет инф.	–	–	+/–	–	–	–
3.	Face Recognition (FACE++)	нет инф.	+	+	+/–	+	–	+
4.	FaceVACS-DBScan (Cognitec Systems)	нет инф.	+	+	+	–	–	–
5.	VeriLook SDK (Neurotechnology)	нет инф.	+	+	–	–	–	–
6.	Каскад-Поток (Техносерв)	нет инф.	+	нет инф.	–	–	–	–
7.	FaceTrack + SideTrack	+/–	нет инф.	нет инф.	нет инф.	+	–	–

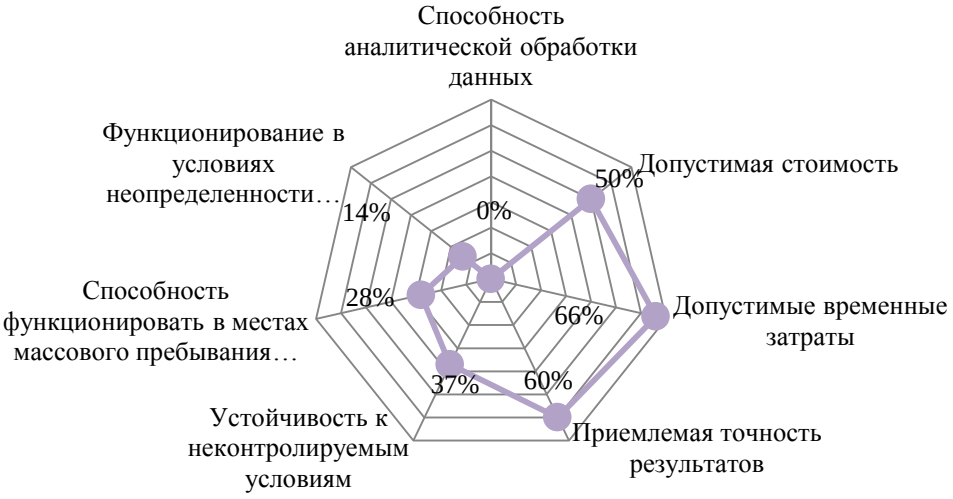


Рисунок 1.1 Процентное распределение реализуемых функций в средствах идентификации при обеспечении безопасности

Вероятности первого и второго рода (FRR и FAR) являются основной характеристикой надежности идентифицирующих систем. Первая ошибка упоминалась выше. Вторая ошибка отражает случаи, когда система распознает человека, на самом деле не являющегося искомым лицом из установленного списка или путает его с другим человеком, – ее принято называть FAR (False Acceptance Rate), положим ее в качестве ошибки второго рода [78].

Устойчивость к неконтролируемым условиям — характеристика, эмпирически оценивающая устойчивость работы системы при различных внешних условиях. Важной характеристикой является скорость работы, она определяет, насколько быстро преступник будет задержан.

Применение высокоскоростных дорогостоящих систем при проведении оперативных мероприятий в условиях, когда оно с участием большого количества людей длятся от нескольких часов до нескольких дней не выгодно. Гораздо удобнее в этом случае воспользоваться существующими системами видеонаблюдения, которые уступают по возможностям системам технического зрения.

1.3 Функционирование систем идентификации по изображению

Большое внимание в технической литературе уделяется рассмотрению принципов работы и созданию на их основе специализированных систем технического зрения. Данные системы могут применяться не только в системах обеспечения безопасности, но также и в других областях. Например, на производстве, для обеспечения деятельности роботов-сборщиков готовой продукции, в промышленной радиографии, или при проведении аэрофотосъемки.

Типовой процесс технического зрения в ИАС можно определить как выделение, идентификацию и преобразование информации из изображений. Его можно разделить на шесть основных этапов: снятие информации, предварительная обработка, сегментация, описание, распознавание, интерпретация ([89], с.9).

Данные этапы с учётом действий оператора приведены на рисунке 1.2. Прокомментируем сами этапы в свете прояснения задач исследования. В данном случае рассматривается только подсистема технического зрения в ИАС.

Снятие информации – получение видеопотока с набором изображений. При этом, учитывая специфику ИАС, можно говорить, что они имеют дело с полутоновыми изображениями или наборами характерных точек в геометрии лиц, которые в состоянии давать применяемые в настоящее время видеокамеры. При этом возможное их улучшение в ходе передачи данных с камеры на объект обработки будет представлять собой действие второго этапа работы ИАС. Часто система сама в состоянии производить подчеркивание границ исследуемого изображения каким-либо способом, например, путем высокочастотной фильтрации.

При дальнейшей машинной обработке на этом этапе используется система улучшения изображения, которая тесно связана с алгоритмами извлечения информации из видеопотока. Процедура улучшения изображений в ИАС часто сводится к выполнению ряда действий для улучшения визуального восприятия изображения оператором. А иногда, если позволяют вычислительные ресурсы, преобразует его в форму, более удобную для визуального анализа.

При проведении машинного анализа изображений возникают задачи третьего этапа. В ходе его проведения решаются задачи сегментации, фильтрации помех, выделения изображений из фона, определение границ объектов. Сегментация, в рассматриваемом случае, – это выделение объектов на лице. В более общем виде, это выделение наборов признаков (характеристик) для определённых классов объектов, которые считаются подклассами какого-то суперкласса.

Описание, четвёртый этап, требует определения значений конкретных признаков (характеристик) для классов объектов, выявленных в ходе сегментации.

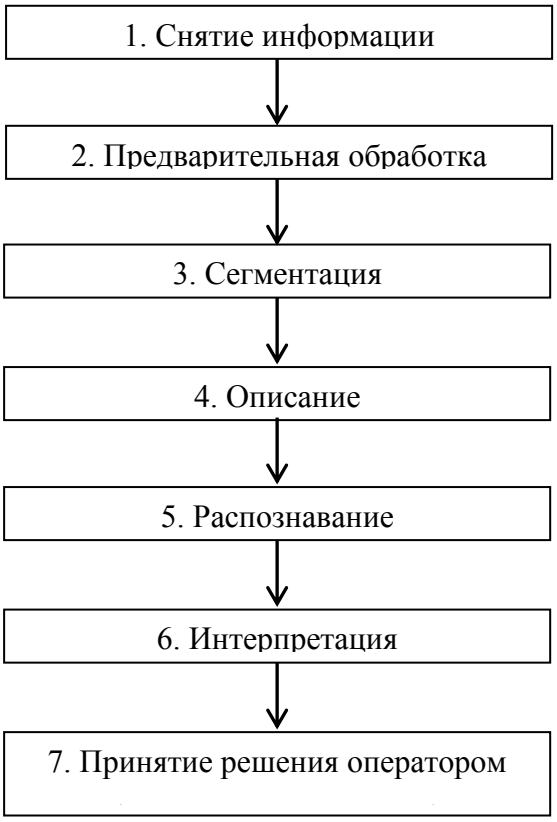


Рисунок 1.2 Алгоритм (этапы) типового процесса технического зрения в ИАС, учётом использования системы оператором

Методы распознавания образов принято делить на группы. Одна из них основана на сравнении полученного набора значений признаков с эталонами. Другая – на понятии систем непересекающихся подмножеств признаков. Следует отметить, что данная группа методов сходна с первой. Ещё одна группа методов распознавания использует понятие конструкции рассматриваемых образов. В результате её применения для описания объекта создаётся список (вектор описаний примитивов). Он содержит информацию об используемых для описания примитивах, входящих в состав объекта, и об их взаимном расположении. В базе данных (БД), или хранилище объектов, хранится набор «эталонов», сходных по структуре описания с объектом распознавания. Для установки факта совпадения (принадлежности к данному классу) выполняются процедуры попарного сравнения списков или, после предварительной сортировки объектов на группы по характерным примитивам, поиска по двоичному дереву.

Обычно получение описаний изображений представляет собой задачу, связанную с перехода от набора признаков изображения, полученных из видеопотока, например, значений яркости, контрастности, положения точек, параметры текстуры, к набору средств описания объекта в виде вектора чисел. Такие наборы чисел требуют значительно меньше вычислительных ресурсов и могут служить в качестве исходных данных для их последующей машинной интерпретации.

Интерпретация на основе распознавания – шестой этап работы системы технического зрения. На этом этапе происходит выявление принадлежности интерпретируемого по группе признаков и их значений объекта к определённой группе распознаваемых объектов, имеющихся в распоряжении системы. Данный этап может осуществляться как автоматически на основе распознавания, так и оператором. Но в большинстве используемых на сегодняшний день ИАС с техническим зрением окончательное решение принимает оператор. И это указано на рисунке 1.2 в качестве 7 этапа.

Кроме того, следует заметить, что «распознавание лица предусматривает выполнение любой из следующих функций: аутентификация - установление подлинности "один в один", идентификация - поиск соответствия "один из многих"» [97]. Данное уточнение необходимо во избежание путаницы в последующих описаниях деталей решаемых задач.

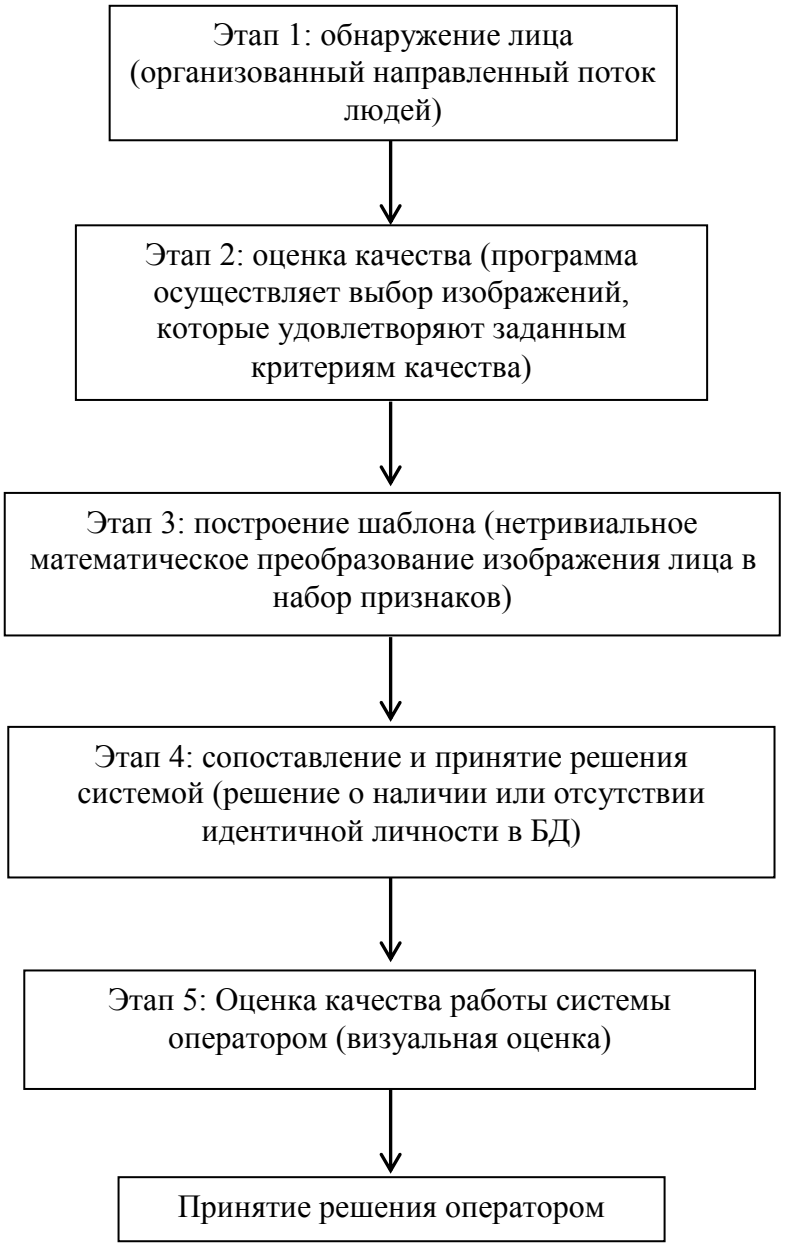


Рисунок 1.3 Алгоритм (этапы) работы системы распознавания лиц

Прежде чем переходить к выводам относительно функций тех или иных систем в отношении их пригодности к решению задач исследования, установим, какие же системы используются в РФ, и как они применяются. Для этого воспользуемся некоторыми обзорами. Так, в частности, в [97] говорится: «В России наибольшее распространение получили такие биометрические движки, как Cognitec (разработка компании Cognitec Systems GmbH, Германия), "Каскад-поток" (разработка компании "Техносерв", Россия), FRS SDK (разработка компании Asia Software, Казахстан), FaceIt (разработка компании L1 Identity

Solutions, США)». Под «движками» в данном случае понимаются системы распознавания лиц, которые в общем случае являются подсистемами комплексных ИАС.

На основе анализа алгоритмов работы этих систем автор [97] делает выводы относительно алгоритма их работы. Для того чтобы увидеть отклонения от такого типового алгоритма, рассмотрим алгоритм работы системы распознавания лиц. Он «в любом биометрическом движке выполняется в несколько этапов: обнаружение лица, оценка качества, построение шаблона, сопоставление и принятие решения» [97]. Алгоритм приведён на рисунке 1.3. Про систему FaceIt было сказано выше, а про Каскад-Поток [97] будет сказано несколько слов далее.

На этапе 1 для качественного съёма информации должны работать организационные меры (например, пропуск людей через пропускной пункт, где они будут задерживаться на небольшое время) и интеллектуальные камеры. Это само по себе накладывает определённый отпечаток на комплексные ИАС, так как значительно увеличивает их стоимость и повышает процент неавтоматического участия людей в процессе. При этом стоимость самой системы не включает в себя стоимости организационных мероприятий и стоимости участия в них дополнительных человеческих ресурсов. Стоимость применения интеллектуальных камер в общей стоимости ИАС также в расчёт не принимается. Предполагается, однако, что данный инструмент снятия информации будет подобно компьютеру выполнять программы для производства метаданных, содержащих сведения о найденных лицах. Каким образом при этом будет организован канал передачи данных на сервер, и как будет осуществляться анализ видео в камерах, автор статьи не говорит. Но очевидно, что камера в этом случае представляет собой вычислительное устройство, не только снимающее информацию и передающее на сервер, но и обрабатывающее видеопоток до его фактической передачи. Клиентское программное обеспечение (ПО) в этом случае выполняется на камере.

Этап 2 очевидно должен выполняться на сервере. Здесь ПО на сервере осуществляет выбор из всего массива детектированных лиц только тех изображений, которые удовлетворяют заданным критериям качества. Критерии качества отбора задаются системе при настройке. Обычно это следующие показатели: ракурс лица (поворот относительно положения «фас» или «профиль», которые есть в БД), размер лица в пикселях (обычно расстояние между зрачками), процент частичного закрытия лица. Но могут задаваться и другие показатели качества отбора.

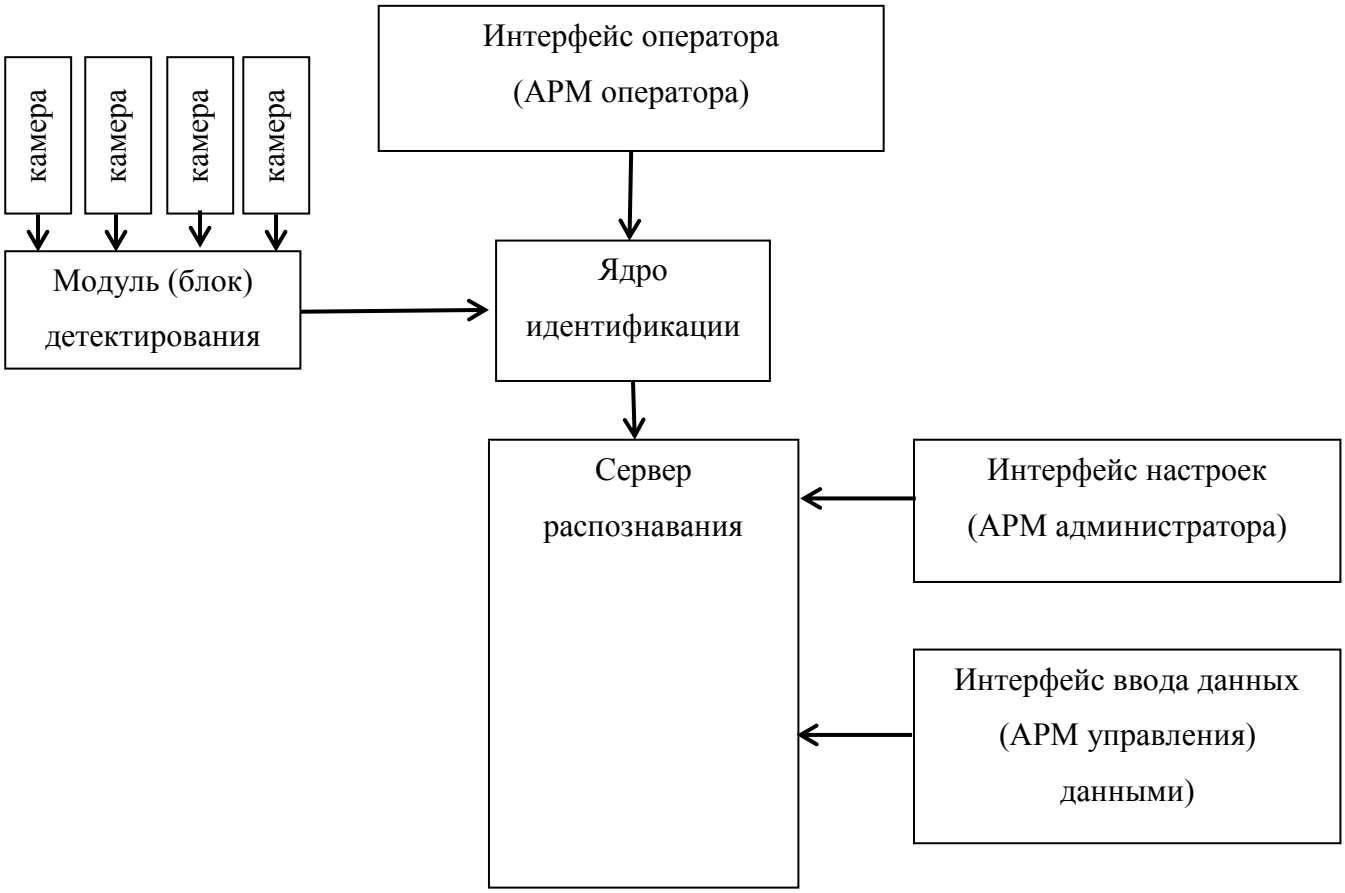


Рисунок 1.4 Архитектура системы «Каскад-поток»

На этапе 3 строится математический шаблон лица (биометрический шаблон). Под ним понимается некоторый набор признаков согласно заложенной в систему математической модели. В зависимости от применяемой системы в нём

используются разные признаки (текстурные свойства лица или его геометрические особенности). Ниже будет приведены некоторые из применяемых

методов для анализа их эффективности в решении поставленных в исследовании задач.

Этап 4 системы распознавания необходим для произведения сравнения построенного по считанному из видеопотока лицу биометрического шаблона с массивом тех шаблонов, которые есть в БД сервера. Этот процесс не может, в принципе, из-за своих требований к вычислительным ресурсам быть реализован на клиенте. Поэтому видимо построение ПО клиента и процесс передачи данных серверу в процессе работы ИАС необходимо внимательно проработать, для того чтобы избежать её перегрузки в процессе эксплуатации.

Пятый этап в работе такой системы связан непосредственно с человеком. Как и в случае с FaceIt, упомянутым выше и описанным в [78], данный этап сопряжён с визуальной оценкой оператором результата работы системы. И здесь можно говорить о том, что без человеческого вмешательства данная система не работает.

Ну и наконец, рассмотрим структуру подсистемы распознавания лиц в ИАС на примере автоматизированной информационно-поисковой системы «Каскад-поток», позволяющей выполнять идентификацию личности по изображению лица, полученного из видеопотока, и поиск человека по БД [49].

Архитектура системы представлена на рисунке 1.4. Система «Каскад-Поток» построена на полностью распределенной сетевой архитектуре, включающей сервер распознавания, блок видеообработки и автоматизированные рабочие места (АРМ) операторов. В состав компонентов системы входят следующие составляющие: модуль детектирования лиц, ядро идентификации, сервер распознавания, АРМ пользователей.

Модуль детектирования лиц обеспечивает автоматическое обнаружение изображений лиц в видеопотоке от источника видеосигнала. Ядро идентификации обеспечивает сравнение изображений лиц, полученных в результате детектирования и размещенных в БД. В результате работы ЯИ формируется рекомендательный список, на основе которого система принимает решение о

личности человека на анализируемом изображении. АРМ системы «Каскад-поток» обеспечивают доступ к функциям системы по мониторингу событий, настройке параметров системы и вводу информации в БД.

Как видно из приводимого близко к тексту [49] описания архитектуры данной системы, в нём не указано при помощи каких биометрических характеристик и с помощью каких алгоритмов «Каскад-поток» осуществляет детектирование. Можно сделать предположение только о том, что в клиенте (модуле детектирования лиц) выполняется преобразование биометрических характеристик лица к виду, удобному для работы ядра идентификации.

Если вернуться к началу описания и вспомнить о физиологических особенностях человека, которые может фиксировать камера (геометрия головы и лица, температурный портрет кожи тела и лица, модель радужной оболочки глаза, форма уха), то можно сделать такой вывод. Большинство используемых в этом направлении в настоящее время систем, упоминаемых в технической литературе, для идентификации одновременно использует для своей работы только шестую часть возможных биологических идентификаторов человека. О применении в комплексных ИАС поиска ПОЛ с помощью анализа поведения, распознавания эмоций, температурный портрет кожи тела и лица пока речь не ведётся. Системы, в которых возможно использование данных признаков, работают отдельно от систем распознавания лиц, а поиск по БД документов возможен только при вводе вручную соответствующего запроса оператором.

Таким образом, применяемые в ИАС подсистемы технического или компьютерного зрения обладают рядом сходных функций, которые можно, обобщив, объединить в единый алгоритм их работы. Однако, в большинстве случаев результатом их работы становится только подготовка данных для принятия решения оператором. Кроме того, они не рассчитаны на работу с большим количеством заданий на распознавание, не обеспечивают распознавание по поведению и не автоматизируют работу остальных подсистем ИАС. В частности в системе «Каскад-поток» данные о лицах вводятся не в процессе

обучения системы, а вручную со специального АРМ. Взаимодействие с другими поисковыми системами, содержащими важные с точки зрения поиска ПОЛ рассмотренные системы также не осуществляют.

Детали работы таких систем определяются вычислительными алгоритмами. Качество данных алгоритмов непрерывно улучшается. Но практика их использования показывает, что есть ряд особенностей их работы, которые пока не позволяют добиваться снижения показателя ошибок первого и второго рода. Поэтому для обеспечения требований реальной жизни в ходе обеспечения массовых мероприятий нужны такие ИАС, которые будут лишены указанных недостатков.

1.3.1 Алгоритмы распознавания лиц

В современном мире, благодаря широкому спектру возможных применений, появился большой интерес к технологиям идентификации человека по лицу. Они используются как в системах обеспечения общественной безопасности: в охранных, контрольно-пропускных системах и системах наблюдения, так и в персональных устройствах – цифровых камерах, роботах-помощниках, смартфонах и ноутбуках. Известно о большом количестве исследований в области идентификации человека по лицу, но на практике, можно сказать, что успешность распознавания зависит от множества факторов: от условий освещенности объекта, угла обзора, возраста человека и маскировочных элементов на нем [137,115]. Все это делает проблему точного распознавания лиц сложной задачей, требующей тщательного изучения.

Как правило, в зависимости от используемых признаков, существующие алгоритмы распознавания лиц подразделяются на три категории:

1. холистические (глобальные) методы – область изображения с лицом представляется вектором высокой размерности, который подается на вход классификатору;

2. локальные методы – для классификации лица выделяются отдельные его геометрические признаки, такие как расположение глаз, носа, рта, щек и т.д.;

3. гибридные методы – совокупность вышеперечисленных методов. По мнению Чжао и др [137], именно объединение локальных и холистических методов может дать наилучший результат в распознавании лиц.

1.3.1.1 Холистические методы

Метод распознавания лиц, основанный на алгоритме вычисления собственных значений – один из холистических методов – впервые появился в 1991 году и впоследствии заслужил всеобщее признание как наиболее эффективный ([129], [112], [119], [106]). В результате этого холистические методы в науке обрели популярность и активно изучаются и поныне. Прежде всего, характерной особенностью холистического подхода к распознаванию лица является то, что она содержит общую информацию о лице человека, а вся область лица представляется вектором с высокой размерностью. Благодаря этому, такое представление отображает общие свойства лиц людей, такие как форма лица и расположение отдельных его элементов относительно друг друга. Известными и эффективными методами холистического анализа, заслужившими популярность, являются метод главных компонент (МГК), линейный дискриминантный анализ Фишера (ЛДА) и анализ независимых компонент (АНК). При использовании АНК происходит поиск статистически независимых базисных векторов и минимизация второго и более высокого порядка зависимостей входных изображений [100]. Рассмотрим более подробно МГК и ЛДА.

1. Метод главных компонент.

МГК является одним из традиционных методов получения ключевых характеристик при распознавании лиц [112]. МГК использует репрезентативную выборку векторов, которая максимизирует дисперсию между характеристиками изображения лица.

Пусть $X = \{X_1, X_2, \dots, X_M\}$ – набор изображений лиц, где $X_j = (x_{1j}, x_{2j}, \dots, x_{Nj})^T$.

Алгоритм МГК заключается в следующем [87]:

a) вычислить центрированную матрицу признаков:

$$X = X - \bar{X}, \tag{1.1}$$

где

$$\bar{X} = \frac{1}{M}\sum_{j=1}^{M} X_j. \tag{1.2}$$

b) далее необходимо найти M ортонормированных собственных векторов u_k, которые наилучшим образом описывают распределение данных в матрице $\bar{X}$. Каждый собственный вектор выбирается таким образом, чтобы максимизировать соответствующее собственное число λ_k:

$$\lambda_k = \frac{1}{M}\sum_{k=1}^{M}({u_k}^T \bar{X}_k)^2. \tag{1.3}$$

Векторы u_k принято называть «собственными лицами». Для их вычисления строится ковариационная матрица:

$$C = cov\,(\bar{X}) = \frac{1}{M}\sum_{j=1}^{M} X_j\,{\bar{X}_j}^T = \bar{X}\,\bar{X}^T. \tag{1.4}$$

3. ковариационная матрица C имеет размерность $N \times N$, а также N собственных чисел и соответствующих им собственных векторов. Отсортировав собственные числа по убыванию, можно выбрать M первых собственных векторов, образующих базис нового пространства признаков.

Таким образом, главные компоненты представляют собой $m \times n$ размерные собственные векторы u_k. Обычно используется до 200 главных компонент. Остальные компоненты кодируют мелкие различия между лицами и шум.

Кроме того «собственные лица», соответствующие вектору, имеет лицеподобный вид.

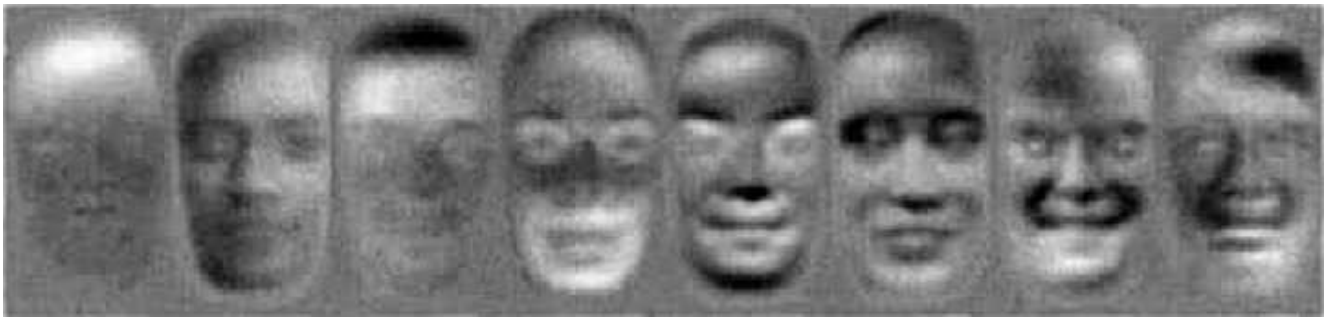


Рисунок 1.5 «Собственные лица» [126]

Полученный на основе обучающей выборки набор собственных векторов используется для представления остальных изображений (рисунок 1.6). Распознавание заключается в сравнении главных компонент неизвестного изображения с компонентами всех остальных изображений.

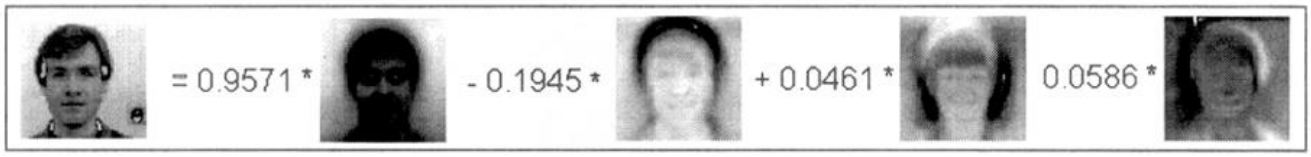


Рисунок 1.6 Портрет, представленный в базисе главных компонент [126]

Считается, что МГК является относительно быстрым, простым и практичным методом, однако он чувствителен к освещенности и изменению ракурса лица на изображении [106]. Таким образом, при его использовании с большими базами данных могут появиться проблемы с точностью. В 3ей главе предложена попытка решения данной проблемы.

2. Линейный дискриминантный анализ Фишера.

В ЛДА используется информация о классах признаков для вычисления набора векторов характеристик лица с минимальным внутрикластерным расстоянием и максимальным межкластерным расстоянием [101].

Далее рассмотрим данный метод [87]. Пусть задано k классов признаков W_1, W_2, … W_k, вычисленных на наборе изображений различных людей, причем $W_i = \{x_{i1}, \dots, x_{imi}\}$, где x_{ij} – вектор признаков длины n, вычисленный для i-ой личности на j-ом изображении, и $m = \sum_{i=1}^{k} m_i$. В рамках ЛДА считается, что векторы признаков обладают нормальным распределением, тогда математическое ожидание для i-го класса выражается следующим образом:

$$\mu_i = \frac{1}{m_i}\sum_{j=1}^{m_i} x_{ij}, \tag{1.5}$$

математическое ожидание всех классов:

$$\mu = \frac{1}{k}\sum_{i=1}^{k} \mu_i, \tag{1.6}$$

матрица внутриклассовой вариативности:

$$\Sigma_w = \frac{1}{m}\sum_{i=1}^{K}\sum_{j=1}^{m_i}(x_{ij} - \mu_i)(x_{ij} - \mu_i)^T, \tag{1.7}$$

матрица межклассовой вариативности:

$$\Sigma_B = \frac{1}{m}\sum_{i=1}^{k} m_i(\mu_i - \mu)(\mu_i - \mu)^T. \quad (1.8)$$

Матрица V для проецирования пространства изображения на пространство признаков выбирается из следующего условия:

$$V_{LDA} = \arg\max_V \frac{|V^T \Sigma_B V|}{|V^T \Sigma_w V|}. \quad (1.9)$$

Оператор V_{LDA} является решением уравнения на собственные числа:

$$\Sigma_w{}^{-1} \Sigma_B v_l = \lambda_l v_l, \quad (1.10)$$

где l є 1…n. Проекция вектора x на подпространство ЛДА осуществляется следующим образом:

$$x = V^T x, \quad (1.11)$$

где V- матрица векторов длины n.

Может существовать до k-1 векторов, составляющих базис пространства признаков. С помощью этих векторов пространство изображений переводится в пространство признаков. По аналогии с методом «собственных лиц» векторы матрицы V называются «лицами Фишера».

Метод ЛДА является достаточно устойчивым к различным условиям освещенности и выражениям лица, но обладает большей трудоемкостью по сравнению с МГК.

1.3.1.2 Локальные методы

До холистических методов, которые появились лишь в последнее десятилетие XX века, активно использовались локальные методы, т.е. алгоритмы выделения отдельных частей лица (глаза, нос и т.д.) [128]. В последнее время локальные методы снова оказались в центре внимания, отчасти из-за их устойчивости к окклюзии и вариациям лица. Окклюзия – это ситуация, в которой два объекта расположены приблизительно на одной линии и один объект, расположенный ближе к камере, частично или полностью закрывает видимость другого объекта. Вариация – изменение объекта распознавания, связанное с изменением ракурса или освещения. У локальных методов существует два преимущества перед глобальными методами [127]. Во-первых, изображение лица

может быть представлено в виде набора векторов отдельных частей лица, что позволяет получить вектора малой размерности. Таким образом, удастся избежать так называемого проклятия размерности[1]. Во-вторых, методы извлечения отдельных частей лица могут быть полезны, когда та или иная часть не видна. Традиционно выделяют следующие основные локальные методы идентификации человека.

1. Сопоставление с эталоном.

Метод заключается в выделении неких эталонных областей лица на изображении и в последующем – сравнение этих областей для двух различных изображений [102].

2. Анализ антропометрических характеристик лица.

Метод основан на выделении и сравнении некоторых антропометрических характеристик лица, таких как толщина бровей над центрами зрачков, ширина лица, расстояние между центром сетчатки правого глаза и точкой кончика носа, и т.д. [84].

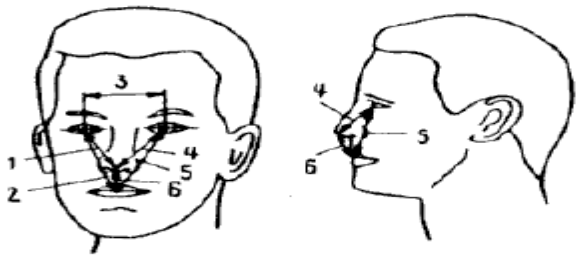


Рисунок 1.7 Антропометрические характеристики лица

3. Методы с использованием фильтров Габора.

Среди всевозможных представленных локальных методов распознавания лиц, благодаря устойчивости к шумам, обусловленным изменением в освещенности, масштабе, сдвиге и вращении [111],[120], вейвлеты Габора были признаны одним из самых лучших локальных методов выделения отдельных частей лица.

- [1] Проклятие размерности — проблема, связанная с экспоненциальным возрастанием количества данных из-за увеличения размерности пространства. Термин «проклятие размерности» был введен Ричардом Беллманом в 1961 году[63].

Окрестность пикселя $a(i, j)$ может быть представлена значениями фильтров Габора. Общий вид фильтра Габора, который характеризуется радиусами эллипса σ_x, σ_y и углом ориентации θ, представлен ниже:

$$h_\theta(x,y) = g_\theta(x,y)\exp(i(x\cos\theta + y\sin\theta)), \quad (1.12)$$

где $g_\theta(x,y)$ является двумерным гауссианом со стандартными отклонениями $\sigma_x\sigma_y$, повернутым на угол θ:

$$g_\theta(x,y) = \frac{1}{\sqrt{\pi\,\sigma_x\sigma_y}}\exp\left(-\frac{(x\cos\theta+y\sin\theta)^2}{2{\sigma_x}^2} - \frac{(-x\cos\theta+y\sin\theta)^2}{2{\sigma_y}^2}\right). \quad (1.13)$$

На основе фильтров Габора предложено много подходов к распознаванию лиц, такие как архитектура динамических связей (АДС) [113], метод гибкого сравнения на графах (МГС)[134], классификатор Габора-Фишера (КГФ) [116], объединение крупномасштабных характеристик Габора (ОКХГ) [135], метод гистограмм локальных бинарных шаблонов Габора (МГЛБШГ)[136]. АДС и МГС это методы представления лиц с использованием согласования эластичных графов. АДС представляет лицо прямоугольным графом с деформируемыми вершинами, соответствующими отдельным чертам лица, полученными с использованием фильтров Габора. Вискотт и соавторы [134] расширили АДС до МГС, используя объектно-адаптированный граф с вершинами, которые соответствуют конкретному лицевому ориентиру. Для распознавания лица Лю и др. [116], применили усовершенствованный линейный дискриминантный анализ Фишера (ЛДАФ) к вектору черт лица, полученному с использованием фильтров Габора, и продемонстрировали, что результат превзошел как МГК, так и ЛДА.

Однако общим недостатком методов распознавания лиц с использованием фильтров Габора является высокая трудоемкость и, следовательно, низкая скорость распознавания [76].

4.Метод сравнения эластичных графов.

В данном методе [33] изображения лиц описываются в виде графов с взвешенными вершинами и ребрами. Вершины графа расположены на ключевых

точках лица, таких как контуры головы, губ, носа и пр., а также на крайних точках элементов лица. Каждое ребро графа помечено расстоянием между вершинами.

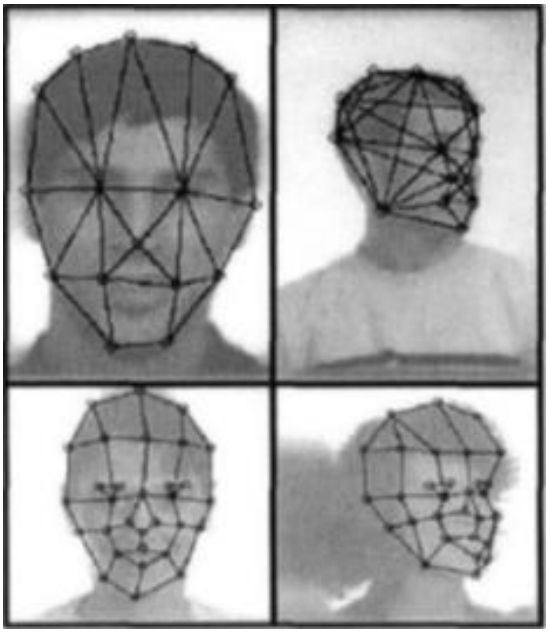


Рисунок 1.8 Пример эластичного графа

Для каждой вершины графа вычисляются джеты. Джеты – комплексные коэффициенты габоровых функций при различных частотах и ориентациях:

$$J_j = a_j \exp(i\varphi_j), \tag{1.14}$$

где аргументы функции a_j и φ_j – есть амплитуда и фаза, определяемые в соответствии с «обстоятельствами» окрестности ключевой точки (яркостью, цветом, контрастностью и т.п.).

Джеты характеризуют локальные области изображения и могут применяться для нахождения точки соответствия заданной области на различных изображениях, а также сравнения соответствующих областей изображений.

Для обнаружения ключевых точек в автоматическом режиме может использоваться обобщенный граф [33].

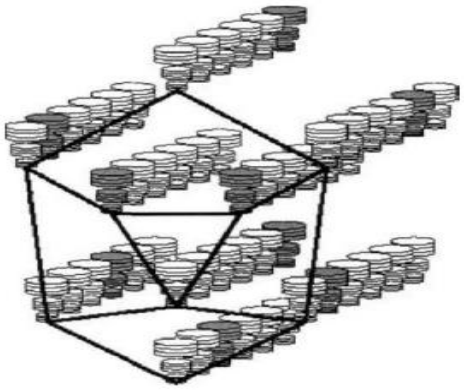


Рисунок 1.9 Обобщенный граф

Пример обобщенного графа представлен на рисунке 1.9. Для построения обобщенного графа необходимо иметь n подготовленных графов, которые отображают структуру человеческого лица. Они могут быть получены путем ручной расстановки точек. Тогда вершинами обобщенного графа будут являться векторы из значений соответствующих вершин каждого из n графов. Ребра обобщенного графа размечены средним значением соответствующих ребер каждого из n графов.

Поиск ключевых точек на изображении неизвестного лица может осуществляться путем вычисления джетов в различных точках и сравнении их с джетами обобщенного графа при помощи функции подобия джетов (1.15).

$$S_a(J,J') = \frac{\sum_j (a_j a_j')}{\sqrt{\sum_j a_j^2 \sum_j a_j'^2}}. \tag{1.15}$$

Процесс распознавания состоит в сравнении графа изображения неизвестного лица с графами изображений известных лиц. Пример функции подобия, которая используется для сравнения графов, представлен ниже:

$$S_{G'}(G,G') = \frac{1}{N}\sum_n \max\left(S_a(J_n,J_n')\right) - \frac{\lambda}{E}\sum_e \frac{(\Delta\overline{x_e} - \Delta\overline{x_e'})^2}{(\Delta\overline{x_e'})^2}, \tag{1.16}$$

где:

- N – количество вершин графа;
- E – количество ребер графа;
- λ – коэффициент относительной важности топографической информации.

Метод эластичных графов считается довольно надежным, однако вычислительно трудоемок. Так, в работе [76] сообщается, что при 95% коэффициенте распознавания на сравнение одного изображения с 87 изображениями тратилось приблизительно 25 с.

4. Метод гистограмм локальных бинарных шаблонов Габора (МГЛБШГ).

Данный метод подразумевает нестатистический подход к распознаванию лиц, сочетающий вейвлеты Габора и локальные бинарные шаблоны (ЛБШ), что повышает репрезентативность пространственной гистограммы. Представление лица с использованием вейвлетов Габора продемонстрировало устойчивость к таким вариациям, как изменение освещения, масштаба, смещение и вращение распознаваемого объекта. В МГЛБШГ используются вейвлеты Габора и ЛБШ для преобразования изображения лица в последовательность гистограмм. Метод заключается в трех шагах.

На первом шаге для получения изображения, называемого «представление вейвлетом Габора» (ПВГ), необходимо выполнить свертку оригинального изображения с фильтром Габора [136]. ПВГ можно получить следующим образом:

$$G_{\mu,v} = f(z) * \varphi_{\mu,v}(z), \quad (1.17)$$

где:

- $f(\cdot)$ − изображение;
- $*$ −оператор свертки;
- φ − фильтр Габора с частотой $v \in \{0, \dots, 4\}$ и ориентацией $\mu \in \{0, \dots, 4\}$.

На втором шаге применяется оператор ЛБШ к ПВГ для получения локальных габоровских бинарных шаблонов (ЛГБШ) изображения. ЛБШ – это оператор, который для извлечения структурных характеристик, перемещает окно размером 3x3 по изображению. Известно, что полученные характеристики устойчивы к изменению освещенности и другим шумам, вызванными различными вариациями [99]. ЛБШ описан ниже.

$$\Gamma(X) = \underset{\forall p \in W}{\otimes} \zeta(\bar{I}(W), I(p)), \tag{1.18}$$

где:

- $\Gamma(X)-$ это двоичная строка, отображающая структурную особенность в окрестности X;
- $\otimes$ – операция конкатенации;
- W – окно размером 3x3;
- $\bar{I}(W)$ – среднее значение интенсивности пикселей в W;
- p – пиксель в окне W;
- $I(p)$ – значения интенсивности пикселя p;
- $\zeta\big(\bar{I}(W), I(p)\big) = \begin{cases} 1, \text{если } \bar{I}(W) < I(p); \\ 0, \text{иначе.} \end{cases}$ – функция сравнения.

Типичный пример оператора ЛБШ представлен на рисунке ниже. Несмотря на простоту оператора ЛБШ, при его использовании для обнаружения и распознания лица демонстрируются хорошие показатели.

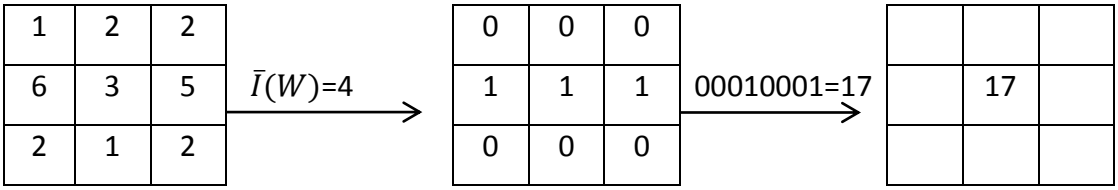


Рисунок 1.10 Пример оператора ЛБШ.

На третьем этапе ЛГБШ изображения разбивается на подобласти 15x15 пикселей. После чего строятся гистограммы подобластей.

Для определения степени схожести двух изображений лиц необходимо сравнить гистограммы, полученные после вышеописанной процедуры – ПГЛГБШ. Сходство между гистограммами эталонного и проверяемого изображений может измеряться посредством расстояния Бхаттачариа (Bhattacharyya), представленного ниже.

$$d_{\text{Bhattacharyya}}(H_1, H_2) = \sqrt{1 - \frac{\sum_I \sqrt{H_1(I) * H_2(I)}}{\sqrt{\overline{H_1}\overline{H_2}N^2}}}, \tag{1.19}$$

где:

- H_1 и H_2 – гистограммы;

- $N-$ общее число интервалов гистограммы;
- $\overline{H}_k -$ определяется следующим образом:

$$\overline{H}_k = \frac{1}{N}\sum_j H_k(j). \quad (1.20)$$

Значение расстояния Бхаттачариа равно 0, если гистограммы в точности одинаковы, и оно стремится к 1 по мере того, как увеличивается уровень различия между гистограммами. Таким образом, за успешно распознанное изображение лица, в соответствии с процедурой МГЛБШГ, можно выбрать проверяемое изображение с наименьшим значением расстояния Бхаттачариа.

1.3.1.3 Гибридные методы

Гибридные методы, включающие как холистические, так и локальные методы, используются для повышения эффективности распознавания. Это достигается благодаря сохранению сильных сторон каждого из них и нивелированию недостатков. В холистических признаках содержится статистическая сводка о пространственных свойствах макета, описывающая глобальные контуры и текстуру изображения. С другой стороны, локальные признаки могут представлять подробные частные свойства.

Пентленд и другие авторы [124] применили принцип «собственных лиц» к некоторым частям лица, таким как глаз, нос и рот, что позволило ввести понятие «собственные глаза», «собственный нос» и «собственный рот». В работе Ланитаса и др.[114] рассматривается гибкая модель внешнего вида распознавания лица, которая использует статистическую информацию о форме лица, а именно активную модель формы (АМФ) и информацию о градации серого; в обоих случаях используется МГК.

В таблице 1.2 приведен сравнительный анализ методов распознавания лица.

1.3.1.4 Вывод

Таким образом, анализ методов идентификации человека на основе уникальности биометрии лица показал, что используемые в настоящее время методы обладают рядом недостатков, связанных, прежде всего, с вычислительной

трудоемкостью и рядом неточностей при распознавании человеческого лица. Использование данных методов в подсистеме технического зрения ИАС сопряжено со сложностями принятия решений оператором как из-за неточности распознавания, так и из-за того, что при увеличении на порядок числа распознаваемых людей система может перестать работать в режиме «реального времени». Кроме того, использование современных методов в существующих системах не позволяет оператору анализировать места пребывания физического лица в прошлом по полученным видеоданным, вести поиск лиц в видеопотоке по фотографиям и решать аналитические задачи.

Основываясь на человеческом зрении, которое использует для распознавания как холистические, так и локальные особенности [128], и построенных математических моделях во 2-ой главе, в 3-ей главе данной работы предлагается вычислительно-эффективный гибридный метод распознавания лиц.

Таблица 1.2 – Сравнительный анализ методов распознавания

Метод / **Характеристика**	**Главных компонент**	**Эластичного графа**	**Антропометрических характеристик лица**	**Сравнения эталонов**	**Линейного дискриминантного анализа**	**МГЛБШГ**
Устойчивость к яркости и контрасту	-	+	-	-	+	+
Устойчивость к незначительному изменению внешности (борода, очки и т.д.)	-	+	-	-	+	+
Устойчивость к изменению ракурса	+	+/-	-	-	-	+
Возможность определения характеристик человека	пол, наличие очков, наличие бороды	пол, наличие очков, наличие бороды	-	-	-	-
Метод сравнения	главные компоненты	функция подобия джетов	метрика	попиксельно	главные компоненты	гистограммы подобластей
Компактный набор характеристик для хранения в БД	главные компоненты	граф, джеты	метрика	фрагменты изображения	главные компоненты	вейвлеты Габора
Преимущества	хранение и поиск изображения в больших БД	способность находить подобные точки	простота идеи	простейший алгоритм сравнения	хранение и поиск изображения в больших БД	высокая точность
Недостатки	неточность при работе с объемными базами данных	вычислительная трудоемкость	сложность выбора совокупности точек, наилучшим образом описывающих человеческое лицо, и надежного нахождения таких точек.	вычислительная трудоемкость	вычислительная трудоемкость	вычислительная трудоемкость

1.3.2 Алгоритмы определения соответствия заданному образу

Далее рассмотрим, как можно автоматически сравнивать между собой такие объекты, как изображения. Внимательно также посмотрим на характер хранения данных об изображениях.

Согласно [44]: «для оценки при помощи ЭВМ сходства или различия объектов, необходимо ввести формальную меру сходства (различия), в терминах которой ЭВМ и будет сравнивать объекты между собой. В задачах распознавания объектов, описываемых наборами ключевых точек, исходная информация представляется в виде конечного множества векторов (дескрипторов) с действительными компонентами» (с.12-13).

Воспользуемся этим источником для того, чтобы уточнить формулы для определения дистанции между объектами распознавания. Будем считать, что входной объект имеет обозначение

$$x \in X = \{x_1, x_2, \ldots, x_r\}, \tag{1.21}$$

где x_1, x_2, …, x_r – характеристики (признаки) входного объекта x, а r – число признаков хранения (и сравнения).

Для хранимых данных выберем обозначение y, при этом

$$y \in Y = \{Y_1, Y_2, \ldots, Y_m\}, \tag{1.22}$$

$$Y_i = \{y^1_i, y^2_i, \ldots, y^r_i\}, \tag{1.23}$$

где Y_1, Y_2, …, Y_m – множество из m хранимых объектов;

m – общее число объектов в БД или их кластеров, представленных одним или несколькими типовыми (средними) объектами хранения;

y^1_i, y^2_i, …, y^r_i – характеристики (признаки) хранимого объекта y;

r – число признаков хранения (и сравнения).

Тогда метрику пространства распознавания, которое строится алгоритмами ИАС при проведении распознавания, будем обозначать как g(x, y).

Наиболее простой и естественный способ задания пространства значений для g(x, y) предположение о его евклидовом характере. Тогда расстояние в нём измеряется как корень квадратный из суммы квадратов разниц значений x и y.

$$g(x, y) = \sqrt{\sum_r (x_i - y^j_i)^2}. \quad (1.24)$$

При этом, разумеется, проводить вычисление расстояния g(x, y) необходимо m раз по числу объектов в БД или их кластеров, представленных одним или несколькими объектами хранения.

Часто для определения расстояний в пространстве изображений приходится использовать более простую метрику. Это связано с сокращением общего количества операций при проведении сравнения. В этом случае расстояние может определяться как сумма модулей разностей между соответствующими признаками

$$g(x, y) = \sum_r |x_i - y^j_i|. \quad (1.25)$$

Иногда необходимо выполнять операцию, обратную операции определения принадлежности входного изображения к данному кластеру (образу). В этом случае расстояние может измеряться по следующей формуле

$$g(x, y) = \sum_r (x_i - y^j_i)^2 . \quad (1.26)$$

Квадраты разности значений характеристик используются как раз для того, чтобы максимизировать общее значение расстояния за счёт наиболее «удалённых» друг от друга признаков.

Для получения более точных данных о соответствии сравниваемых изображений друг другу уместно вводить в расчёт расстояния весовые коэффициенты для каждого из признаков. Тогда формула для его расчёта имеет следующий вид

$$g(x, y) = \sqrt{\sum_r \gamma_i (x_i - y^j_i)^2} \quad . \quad (1.27)$$

При этом вычисление коэффициентов γ_i обычно связано с получением оценок экспертов. Поэтому зачастую γ_i имеют вид оценок

$$\gamma_i \in Ÿ = \{Ÿ_1, Ÿ_2, \ldots, Ÿ_K\}, \tag{1.28}$$

и

$$\gamma_i = 1/K \left(\sum_K Ÿ_i \right). \tag{1.29}$$

Задание весовых коэффициентов расстояний между объектами требует априорной информации о них. А оценки экспертов или не всегда дают нужную точность, или невозможны в принципе. Поэтому целесообразно измерять значения в расстояниях между объектами по таким формулам, в которых возможно выравнивание весов в слагаемых от различных признаков объектов. Это особенно актуально, если веса или их оценки имеют значительный разброс по значениям. Для этого, например, можно использовать расстояние по Камберу. Принимая уже введённые ранее обозначения, формула для расчёта расстояния принимает следующий вид

$$g(x, y) = \sum_r |x_i - y^j_i| / |x_i + y^j_i| . \tag{1.30}$$

Формулу уместно применять в случае необходимости масштабных изменений (резкого увеличения или резкого уменьшения) изображения, в котором будут сохранены основные отличительные признаки идентификации (например, главные компоненты).

Если предположить, что значения получены как значения функций

$$x \in X = \{ v_1(x), v_2(x), \ldots, v_r(x) \}, \tag{1.31}$$

$$y \in Y = \{ z_1(y), z_2(y), \ldots, z_r(y) \}, \tag{1.32}$$

где $v_i(x)$, $z_i(y)$ – значения некоторых функций (например, показания датчиков), и при этом

$$v_i(x) = \{R^n \rightarrow R^1\} , \tag{1.33}$$

$$z_i(y) = \{R^n \rightarrow R^1\} , \tag{1.34}$$

то расстояние между объектами X и Y можно рассчитать по формуле Чебышева

$$g(v(x), z(y)) = \max_i | v_i(x) - z_i(y) |. \quad (1.35)$$

Аналогом евклидовой метрики является метрика «городских кварталов» или манхэттенская метрика, определяемая как разность модулей «координат» (значений признаков в многомерном пространстве) сравниваемых объектов. Характерной её чертой является то, что для неё сглаживаются большие отличия в значениях признаков. Формула для такой метрики в наших обозначениях будет выглядеть так

$$g(x, y) = \sum_r (|x_i| - | y^j_i|). \quad (1.36)$$

Иногда для поиска нужного кластера удобно использовать метод от противного или искать те объекты, которые точно не совпадают с тем, который поступил на вход МД ИАС. Тогда необходимо вести расчёт расстояния исходя из числа «несовпадений» значений признаков. Для этого удобно использовать формулу вычисления расстояния по Хеммингу

$$g(x, y) = 1/R \left(\sum_r (x_i - y^j_i)^2\right). \quad (1.37)$$

Перечисленные выше методы получения данных о соответствии входных объектов хранимым принято называть детерминистскими. Помимо детерминистских методов в определении расстояний между объектами в распознавании могут использоваться статистические методы.

Одним из них служит так называемый метод «ближайшего соседа». Для прояснения метода необходимо установить связь между отнесением объекта к тому или иному кластеру (образу) и вероятностью ошибки при решении этой задачи. Обычно в рамках решения такой задачи необходимо определить апостериорную вероятность принадлежности объекта x образу Y_i при условии, что признаки этого объекта имеют значения $x_1, x_2, \ldots, x_r$.

Фактически для этого вокруг распознаваемого объекта x строится ячейка объёма $\forall$. Неизвестный объект относится к тому образу, число сходных объектов которого из имеющихся Y_i в этом объёме оказалось большинство. Т.е. число

объектов образа x, попавших в окрестность x, даёт оценку усреднённой по объёму $\forall$ плотности вероятности $p(Y_i,/x)$.

Для прояснения определения расстояния, рассчитываемого статистическими методами, необходимо определить обучающую выборку. Так как ИАС изначально не знает, к какому объекту отнести входной, то она начинает сравнивать с имеющимися. Когда выясняется, что среди них нет того, который удовлетворяет требованиям «схожести» (решающее правило даёт значение для расстояния между всеми хранимыми и входным образами меньше или больше заданного порога), начинается построение нового кластера. Для этого необходимо несколько объектов из данного кластера, которые и будем называть обучающей выборкой. Другие детали данного определения можно почерпнуть в технической литературе по распознаванию образов и кластерному анализу ([10], [35], [38], [9], [15], [24], [27], [50], [95], [96]).

Рассмотрим ситуацию, когда у нас есть обучающая выборка $\varkappa_1, \varkappa_2, \ldots, \varkappa_r$.

$$\varkappa_i = \{ \varkappa^i_1, \varkappa^i_2, \ldots, \varkappa^i_r \}, \tag{1.38}$$

для которой известно, что

$$\varkappa_i \in Y = \{ Y_1, Y_2, \ldots, Y_m \}, \tag{1.39}$$

где Y – образы в ЦБД ИАС.

Тогда вероятность того, что x попадёт в объём $\forall$ для класса $\varkappa_i$

$$P(\forall/x) = \forall * p(\varkappa_i,/x), \tag{1.40}$$

если окрестность $\varkappa$ слишком мала и в ней $p(\varkappa_i,/x) = const$, или

$$P(\forall/x) = \int p(\varkappa_i,/x)\, d\forall, \tag{1.41}$$

для остальных случаев.

Это и есть вероятность того, что x будет распознан как Y_i или $P(Y_i/x)$. Тогда, для определения расстояния между распознаваемым и хранимыми объектами по Байесу, необходимо выбрать максимальную апостериорную вероятность того, что x будет распознан как Y_i.

$$P(Y_i/x) = \max_j P(\varkappa_j,/x). \tag{1.42}$$

Использование различных методов в распознавании позволяет достаточно полно исследовать входной объект с МД, но при этом комбинирование различных методов внутри одной ИАС приводит к большим вычислительным затратам. А это, в свою очередь, сильно снижает её скоростные возможности и нагружает оператора. Поэтому целесообразно стремиться к тому, чтобы ИАС использовала только один из заданных алгоритмов распознавания.

Таким образом, используя для получения данных о соответствии объекта заданному образу различные методы вычисления расстояния, возможно получить нужный результат при распознавании. Вопрос обоснованности применения того или иного метода решают обычно производители ПО ИАС.

Для повышения оперативности работы ИАС с оператором в реальном времени в реальном времени необходимо использовать ряд новых алгоритмов.

1.3.3 Алгоритмы обнаружения пожара

В настоящее время для детектирования пожара или дыма используются два основных подхода [32]:

1. Подход, использующий методы, основанные на анализе яркостной и цветовой составляющей изображения.

Для использования этого подхода необходимо задать модель, описывающую «пожар» или «дым». Модель может принадлежать одному из трех типов: классификаторы, структурные, параметрические.

Для работы классификатора необходимо сформировать достаточно большое количество эталонов, что является весьма трудоемкой задачей, поскольку у пламени или дыма существует практически бесконечное множество вариаций. Структурные модели тоже не вполне подходят для решения данной задачи, так как объект моделирования не является структурным. Таким образом, сейчас в основном используются параметрические модели, характеризующиеся определенным статическим или динамическим цветовым описанием.

Недостатком данного подхода является сложность идентификации пламени на дальнем расстоянии [94].

2. Подход, основанный на использовании опорных изображений, полученных до наступления деструктивного события при различных условиях освещенности. Основной принцип заключается в выделении очагов пожара путем вычитания последовательных кадров или фонового изображения.

Основным недостатком данного подхода является то, что перекрывающие друг друга области на изображениях могут быть ошибочно приняты в качестве фона.

Автор полагает целесообразным использовать комбинированный метод, сочетающий в себе перечисленные выше подходы. На первом шаге анализа предлагается использовать второй подход, в случае неопределенности дополнительно применять первый.

1.3.4 Алгоритмы отслеживания траектории движения

После того как человек был идентифицирован как лицо потенциально опасное, может возникнуть необходимость анализа его действий и мест пребывания, с кем будет встречаться, и т.д. Поскольку запись видеопотока может осуществляться с различных камер и в течение большого промежутка времени, то для непосредственного просмотра потребуются значительные человеческие ресурсы. Стоит заметить, что сотрудника службы безопасности о событиях следует оповещать только один раз, чтобы не дублировать одинаковые сообщения с разных камер также необходимо отслеживать траектории движения объектов. Из этого следует необходимость автоматического отслеживания интересуемых объектов.

Для решения задачи отслеживания движения объектов можно воспользоваться следующими методами: шаблонов движений [121], сдвига среднего [121]; непрерывно адаптирующегося сдвига [133], Виолы – Джонса [3], Лукаса – Канаде [133].

В таблице 1.3 приведен сравнительный анализ указанных методов.

Для экономии вычислительных ресурсов, стоит проводить отслеживание только тех объектов, которые уже были идентифицированы как представляющие интерес для сотрудников службы безопасности. Поэтому необходимо выбрать метод отслеживания без непосредственного поиска объекта, таковыми является, методы сдвига среднего, непрерывно адаптирующегося сдвига и Лукаса – Канаде.

Особенностью видеоданных, используемых для видео регистрации событий в местах скопления людей, является удалённость объекта слежения без использования оптического и программного средства увеличения. Это приводит к значительному уровню шумов и оптических иллюзий, и не все алгоритмы устойчивы к данным условиям. Наименьшей ошибкой потери фокуса на объекте во время отслеживания из данных алгоритмов обладает алгоритм Лукаса – Канаде (7%) [2]. Но в данном методе существует проблема, связанная с тем, что когда объект выходит из кадра или заходит за некоторое препятствие, отслеживание продолжается не за первоначальным объектом, а за некоторой областью на кадре.

Одной из основных проблем применения метода отслеживания движения является его согласованное применение в наборе видеопотоков с нескольких камер. В ситуации, когда человек может попасть одновременно в объектив нескольких камер и когда человек переходит из поля видимости одной камеры в поле видимости другой камеры, необходимо формировать один видеопоток с траекторией движения объекта.

Таким образом, проведённый в подразделе анализ методов поведения человека показал, что применяемые в настоящее время методы обладают рядом недостатков, среди которых затруднение в работе ИАС в условиях большого количества камер и отсутствие возможности идентификации личности и отслеживания человека по фотографии с применением дополнительной информации. Поэтому целесообразна разработка соответствующих алгоритмов и структур данных, которые позволят в будущем реализовать данную возможность.

Таблица 1.3 – Сравнительный анализ методов отслеживания движения объекта

Метод / Характеристика	**Шаблонов движений**	**Сдвига среднего**	**Непрерывно адаптирующегося сдвига**	**Лукаса – Канаде**	**Виолы – Джонса**
Граничные точки вектора движения	граница объектов	центр масс точек, определяющих объект слежения	центр масс точек, с автоматическим подстраиванием границы и размера окна, в пределах которого расположен объект слежения	набора пикселей, полученных с помощью дифференциального вычисления оптического потока	наборов пикселей, совпадающих с заранее подобранными шаблонами
Автообучение	+	+	+	+	-
Автоинициализация объекта слежения	+	-	-	-	+
Устойчивость при быстром движении объекта	-	-	-	-	+
Устойчивость к незначительному цветовому отличию объекта слежения от фона	+	-	-	+	+
Устойчивость к подвижному фону	-	+	+	+	+
Устойчивость к изменению размеров объекта от времени	+	-	+	-	+
Преимущества	автоинициализация объекта слежения	устойчивость к подвижному фону	устойчивость к изменению размера отслеживаемого объекта	высокая эффективность	высокая эффективность
Недостатки	высокая вероятность захвата участка фона вместо объекта	отслеживаемый объект должен иметь четкую цветовую границу с фоном	отслеживаемый объект должен иметь четкую цветовую границу с фоном	необходимость инициализации объекта слежения	вычислительная трудоемкость обучения

1.4 Моделирование нарушителя в системе безопасности

Для обеспечения безопасности места массового пребывания людей необходимо противостоять нарушителю. При определении нарушителя стоит разделять внешних и внутренних.

Под внешним нарушителем понимается лицо (группа лиц), находящееся в общественном месте, потенциальной целью которого является совершение преступления. При этом в хранилище ИАС содержится фотография данного нарушителя. Примерами внешних нарушителей являются: специальные службы иностранных государств, террористические и экстремистские группировки, криминальные структуры, конкурирующие организации. При проникновении на объект нарушителя данного типа служба безопасности должна обнаружить и своевременно среагировать. Повысить эффективность обеспечения безопасности общественного объекта предполагается путем применения ИАС.

Внутренние нарушители – лица, имеющие право постоянного или разового доступа к хранимым персональным данным физических лиц в БД ИАС. Примерами внутренних нарушителей являются: администраторы ИАС, операторы ИАС, лица, привлекаемые для пусконаладочных работ, лица, обслуживающие инфраструктуру. Данные нарушители, например, в результате подкупа, могут получить несанкционированный доступ к персональным данным интересантов с целью их изменения или передачи третьим лицам. Следовательно, в ИАС должно быть реализовано сохранение информации о действиях пользователя в электронный журнал.

Классификация нарушителей с указанием их вида, типа, потенциала, возможных угроз и возможностей приведены в таблице 1.4 и на рисунке 1.11. Данная классификация позволяет спроектировать систему безопасности, устойчивую к указанным угрозам. При классификации нарушителей использовалась методика определения угроз безопасности информации [39].

Таблица 1.4 - Классификация нарушителей

№	Вид нарушителя	Тип нарушителя	Потенциал нарушителя	Возможные угрозы	Возможности нарушителя
1.	Специальные службы иностранных государств	Внешний, внутренний	Высокий	Нанесение ущерба государству. Дискредитация или дестабилизация органов государственной власти и организаций	Обладают всеми возможностями нарушителей со средним потенциалом. Имеют хорошую осведомленность о системах безопасности. Могут использовать недостатки системы безопасности и применять средства маскировки.
2.	Террористические и экстремистские группировки	Внешний	Средний	Нанесение ущерба государству. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций	Обладают всеми возможностями нарушителей с низким потенциалом. Проинформированы об организационно-технических методах и недостатках функционирования системы безопасности данного типа. Могут применять устройства техногенного характера для совершения теракта.
3.	Криминальные структуры	Внешний	Средний	Причинение имущественного ущерба.	Обладают всеми возможностями нарушителей с низким потенциалом. Проинформированы об организационно-технических методах и недостатках функционирования системы безопасности данного типа.
4.	Физические лица	Внешний	Низкий	Идеологические или материальные мотивы. Причинение имущественного ущерба.	Могут получить информацию о функционировании средств безопасности из открытых источников, а также о преодолении средств защиты.
5.	Конкурирующие организации	Внешний	Средний	Получение конкурентных преимуществ. Причинение имущественного ущерба.	Обладают всеми возможностями нарушителей с низким потенциалом. Проинформированы об организационно-технических методах и недостатках функционирования системы безопасности данного типа.

6.	Лица, обслуживающие инфраструктуру	Внутренний	Низкий	Причинение имущественного ущерба. Получение доступа к персональным данным интересантов из любопытства или с целью извлечения материальной выгоды. Непреднамеренные или неквалифицированные действия.	Могут получить информацию о функционировании средств безопасности из открытых источников, а также о преодолении средств защиты.
7.	Лица, привлекаемые для пусконаладочных и иных видов работ	Внутренний	Средний	Причинение имущественного ущерба. Получение доступа к персональным данным интересантов. Неквалифицированные действия. Нарушение функционирования систем безопасности.	Обладают всеми возможностями нарушителей с низким потенциалом. Проинформированы об организационно-технических методах и недостатках функционирования системы безопасности данного типа. Обладают глубокими познаниями о технической составляющей систем безопасности.
8.	Операторы систем безопасности	Внутренний	Средний	Причинение имущественного ущерба. Получение доступа к персональным данным интересантов. Неквалифицированные действия. Сокрытие тревожного события. Нарушение функционирования систем безопасности.	Обладают всеми возможностями нарушителей с низким потенциалом. Проинформированы об организационно-технических методах и недостатках функционирования системы безопасности данного типа. Обладают непосредственным доступом к системам безопасности.
9.	Администраторы систем безопасности	Внутренний	Высокий	Причинение имущественного ущерба преступным путем. Получение доступа к персональным данным. Неквалифицированные действия. Нарушение функционирования систем безопасности.	Обладают всеми возможностями нарушителей со средним потенциалом. Обладают доступом к системам безопасности для внесения закладок. Имеют хорошую осведомленность о системах безопасности. Обладают возможностью использования недостатков системы.

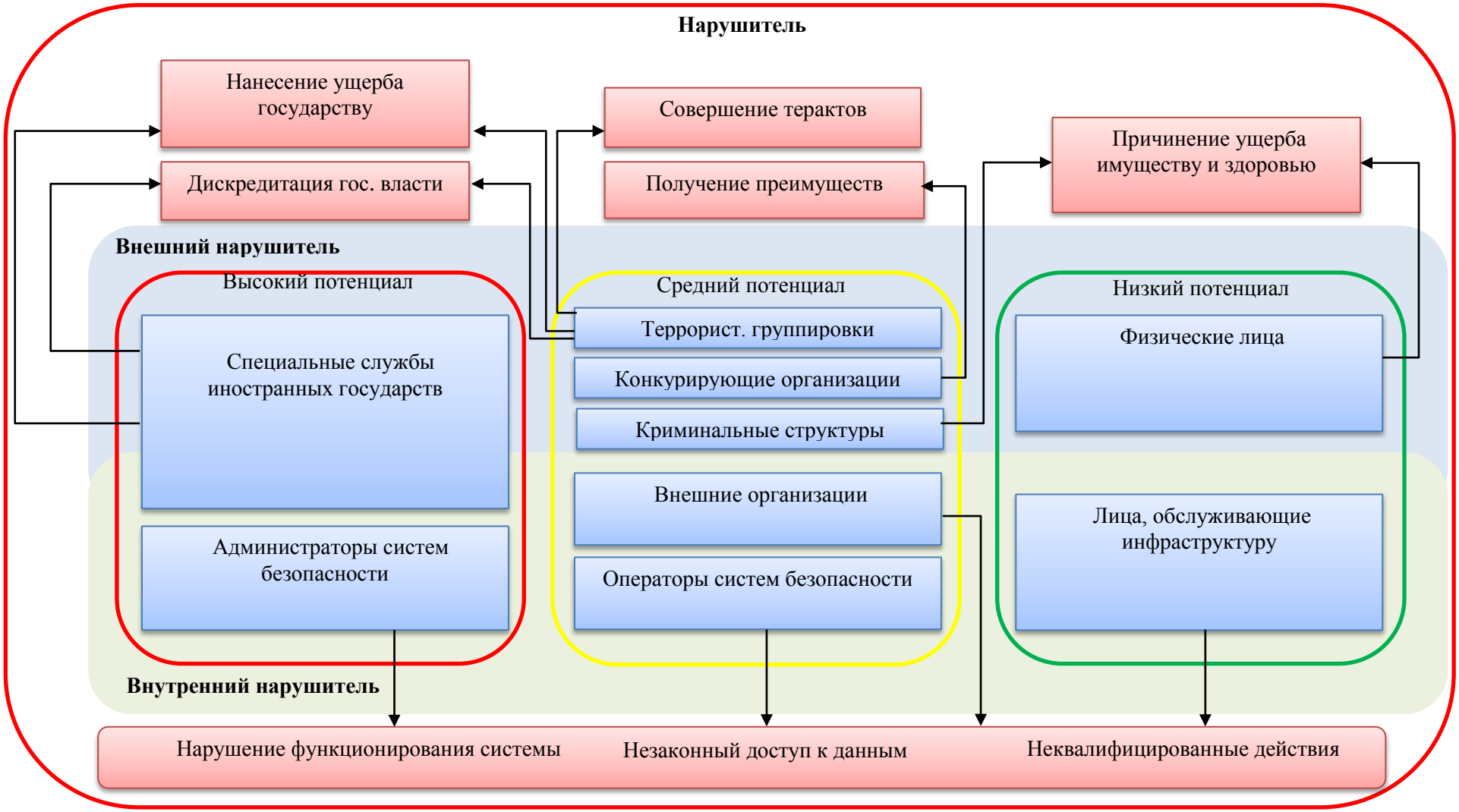


Рисунок 1.11 Нарушитель в системе обеспечения безопасности

1.5 Вывод по первой главе

Одним из основных мест общественно-опасных преступных проявлений криминальных структур и террористических группировок являются места массового пребывания людей.

В результате анализа определено, что защищенность мест массового пребывания людей при эффективном и экономном использовании сил и средств может быть повышена за счет использования информационно-аналитической системы поддержки управления безопасностью, которая обеспечивает предоставление информации для координации сил и средств охраны при проведении мероприятий прогнозирования, обнаружения и противодействия дестабилизирующим проявлениям интересантов.

Проведен анализ и определено распределение функциональных возможностей отечественных и зарубежных систем данного вида. В результате анализа выявлена практическая невозможность использования функций существующих решений для комплексной и оперативной поддержки управленческих решений, в условиях неопределенности информации при неконтролируемой обстановке в местах массового пребывания людей.

Применяемые в подсистемах распознавания алгоритмы работы систем компьютерного зрения и их аналогов обладают рядом сходных функций, которые можно, обобщив, объединить в единый алгоритм работы. Кроме того, в большинстве случаев результатом их работы становится только подготовка данных для принятия решения.

На основе полученных результатов в настоящее время актуальным является вопрос разработки моделей и алгоритмов информационно-аналитической поддержки управления безопасностью в местах массового пребывания людей на базе автоматизированных средств дистанционной идентификации по изображению.

Следовательно, направление дальнейшего исследования будет заключаться в следующем:

1. Разработке многопараметрической модели поддержки управления безопасностью мест массового пребывания людей, оборудованных средствами идентификации по изображению, на основе синтеза различных математических методов.

2. Разработке вероятностной оценки эффективности функционирования системы безопасности, в котором в совокупности необходимо учесть скорость реакции персонала на событие деструктивного характера, переменную скорость движения нарушителя, нагрузку сети видеоконтроля, объем хранимой информации в базе данных, количество анализируемых нарушителей и другие параметры автоматизированной системы идентификации по изображению.

3. Разработке алгоритмов формирования и управления безопасностью мест массового пребывания людей, оборудованных средствами идентификации по изображению.

4. Разработке и реализации в программном обеспечении алгоритмов функционирования и архитектуры системы поддержки управления безопасностью на основе компьютерного зрения с учетом полученной модели.

5. Разработке рекомендаций по определению степени пригодности кандидата к работе в службе безопасности с учетом индивидуальных особенностей.

6. Оценке финансово-экономического эффекта системы автоматизированной идентификации по изображению.

ГЛАВА 2. РАЗРАБОТКА МОДЕЛИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ПОДДЕРЖКИ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

Данная часть диссертационной работы посвящена разработке модели поддержки управления безопасностью мест массового пребывания людей, оборудованных средствами идентификации по изображению, на основе которой будет получена вероятностная оценка эффективности функционирования системы безопасности, в которой впервые в совокупности учитываются скорость реакции персонала на событие деструктивного характера, переменная скорость движения нарушителя, нагрузка сети видеоконтроля, объем хранимой информации в базе данных, количество анализируемых нарушителей и другие параметры автоматизированной системы идентификации по изображению.

Кроме того на основе данной модели будет получен алгоритм формирования безопасности мест массового пребывания людей учитывающие особенности охраняемых объектов и средств идентификации по изображению.

2.1 Модель управления безопасностью

Для моделирования системы безопасности введем определения составляющих.

Объект управления – это система безопасности места массового скопления людей, оборудованного комплексом технических средств идентификации по изображению.

Субъект управления – это управляющая система (орган управления).

Далее выстроим модель с учетом подходов [41], [8], [46], [88], [1]. Будем считать, что состояние объекта управления (данной системы безопасности) описывается вектором $y \in Y$ и Y – множество возможных состояний объекта. Значение y зависит от управляющих воздействий на объект $u \in U$ и дестабилизирующих факторов внешней среды $x \in X$. При этом множество

состояний (Y) включает активную (Y_1) и пассивную (Y_2) составляющие системы безопасности: $Y = Y_1 \times Y_2$.

Под активной составляющей объекта управления (Y_1) подразумеваются сотрудники службы безопасности, которые обладают свободой выбора своего состояния, собственными целями и интересами. Таким образом при выборе управляющего воздействия на активную составляющую необходимо учитывать состояние сотрудников, возможность самостоятельного выбора состояния и их индивидуальные особенности.

Пассивная составляющая объекта управления (Y_2) представляет собой комплекс технических средств безопасности. В данной работе рассматривается только комплекс технических средств идентификации по изображению. Особенностью данной составляющей является детерминированность, отсутствие свободы выбора своего состояния.

Будем считать, что состояние пассивной составляющей в основном определяется следующими параметрами:

- точностью идентификации по изображению;
- скоростью;
- количеством анализируемых интересантов;
- нагрузкой сети видеоконтроля;
- объем хранимой информации в базе данных и т.д.

Примерами дестабилизирующих факторов внешней среды являются:

- криминальные явления – воздействия нарушителя на функционирование места массового пребывания людей;
- природные явления – ураганы, аномальные температуры, землетрясения и т.д.;
- техногенные явления – аварии, катастрофы и т.д.;
- социально-политические явления – социальные волнения, военные действия и т.д.

Таким образом [5], объект управления можно описать уравнением вида $\Theta(t) = \Phi[Y(t), U(t), X(t), t]$. В результате управленческих воздействий $U(t)$, внешних факторов $X(t)$ при начальном условии $Y(t_0)$ в фазовом пространстве управления состояние объекта меняется, и решение уравнения имеет вид $Y(t, U(t), X(t), y(t_0))$. Каждому состоянию объекта (решению уравнения) соответствует определенная точка. Соединяющую эти точки кривую называют траекторией движения объекта.

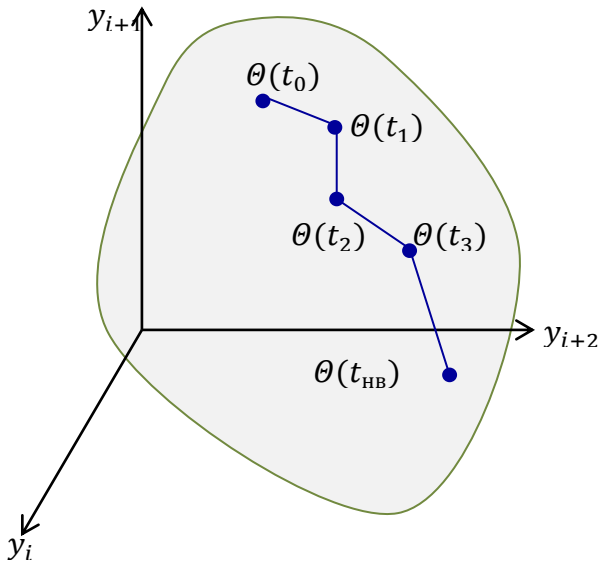


Рисунок 2.1. Фазовое пространство управления для трех переменных состояний

Предположим, что в области Θ можно выделить некоторую подобласть состояний Θ_c, которая является желательной. Тогда цель управления заключается в том, чтобы перевести объект из начального состояния $Y(t_0)$ в конечное состояние $Y(t_k)$, принадлежащее Θ_c. Задача управления заключается в том, чтобы в области допустимых управлений подобрать такое управляющие воздействие, при котором достигнута цель. То есть требуется отыскать такое допустимое управление $U(t)$, определенное на временном отрезке $[t_0, t_k]$, при котором уравнение объекта при заданном начальном состоянии и известном векторе $X(t)$ имеет решение $Y(t)$, удовлетворяющее ограничению $Y(t) \in \Theta(Y)$ при всех $t \in [t_0, t_k]$ и конечному условию $Y(t_{нв}) \in \Theta_c$.

Далее рассмотрим модели функционирования ИАС.

2.2 Влияние объема данных на систему поддержки управления

При рассмотрении ИАС далее по тексту будем рассматривать только те из них, которые модули видеодетектирования которых основаны на анализе лиц.

Данный метод идентификации ближе всего к теме исследования. Все ИАС, содержащие подобный модуль видеодетектирования, работают на основе распознавания образов. В их состав помимо указанного модуля включают обычно программные средства, называемые «ядром идентификации» (ЯИ) и хранилище, содержащие ЛБШ или иные шаблоны, данные из которых использует ЯИ.

Модуль детектирования лиц обеспечивает автоматическое обнаружение изображений лиц в видеопотоке от источника видеосигнала. В ядре идентификации осуществляется сравнение изображений лиц, полученных в результате детектирования и размещенных в хранилище. В рамках работы в качестве хранилища рассматривается как база данных, реализуемая на основе одного из существующих решений в области систем управления базами данных, так и оперативная память сервера. В результате работы ЯИ формируется рекомендательный список, на основе которого оператор ИАС принимает решение о личности на анализируемом изображении.

Существует несколько типов ИАС, классифицируемых по типу хране-ния данных о распознаваемых людях. Первый тип связан с наличием у ИАС специального хранилища, содержащего информацию о шаблонах лиц, например в виде локальных бинарных шаблонов (ЛБШ) ([99]). Для идентификации человека необходимо произвести сравнение шаблона лица распознаваемого человека с шаблонами в хранилище.

В другом типе ИАС, предполагается, что биометрическая информация и ее «шаблон хранятся на карте, которая всегда под контролем владельца» [51]. Соответственно, при идентификации человека необходимо осуществить проверку наличия заданной информации в хранилище ИАС по адресу, указанному в предъявляемой карте.

Для эффективного использования ИАС необходимо, чтобы реакция системы соответствовала требуемому уровню. С целью оценки скорости реакции ИАС рассмотрим временные характеристики при обработке запросов. Под запросом будем понимать сформированное обращение ИАС к хранилищу на

идентификацию человека. Скорость обработки запросов и объем данных имеют обратную зависимость.

Время обработки *n* запросов можно посчитать по следующей формуле:

$$t_{\text{в-обр}} = n * t_{\text{обр}}, \quad (2.1)$$

где

- $t_{\text{в-обр}}$ – время обработки всех *n* запросов (от одного или более модулей видеодетектирования);
- $t_{\text{обр}}$ – время обработки одного запроса,

при этом

$$t_{\text{обр}} = t_{\text{рег}} + t_{\text{ш}} + t_{\text{выб}} * m, \quad (2.2)$$

где

- $t_{\text{рег}}$ – время, затраченное на регистрацию объекта (выделение лица из видеопотока и формирование фотопортрета интересанта);
- $t_{\text{ш}}$ – время предобработки (формирование шаблона лица) для дальнейшего анализа его средствами поиска в хранилище;
- $t_{\text{выб}}$ – время формирования данных из хранилища по запросу ЯИ, передачи их и сравнения по очередной записи из хранилища.

В случае хранения шаблона на карте интересант предъявляет данный носитель информации. На карте хранится информация о шаблоне и сведения об адресе шаблона в хранилище, с которым необходимо произвести сравнение. Без ограничения общности будем полагать, что в этом случае время регистрации, предобработки и формирования данных то же, что при идентификации человека на основе биометрии лица. Однако, для данной ИАС не требуется осуществления поиска, достаточно обратиться к хранилищу по адресу, указанному на карте. Тогда при предъявлении карты с информацией о шаблоне формула (2.2) представляется следующим образом:

$$t`_{\text{обр}} = t_{\text{рег}} + t_{\text{ш}} + t_{\text{выб}}, \quad (2.3)$$

при этом отношение $T_{соб}$ скорости обработки для разных типов ИАС определится так:

$$\mathrm{T}_{\mathrm{соб}} = \frac{t'_{\mathrm{обр}}}{t_{\mathrm{обр}}} \quad (2.4)$$

или

$$\mathrm{T}_{\mathrm{соб}} = \frac{t_{\mathrm{рег}} + t_{\mathrm{ш}} + t_{\mathrm{выб}}}{t_{\mathrm{рег}} + t_{\mathrm{ш}} + m * t_{\mathrm{выб}}}. \quad (2.5)$$

Далее $T_{соб}$ будем называть относительной реакцией системы (ОРС). Представим ОРС параметром ИАС, используемым для количественной оценки времени ее работы по единичному запросу. Фактически ОРС – это зависимость времени обработки единичного запроса (запроса, содержащего данные на одного интересанта) от количества записей в хранилище. Иными словами ОРС – это скорость реакции на запрос к хранилищу. Под хранилищем подразумевается как центральная БД или ее локальные «продолжения» в виде определенных локальных БД, так и оперативная память, используемая для повышения оперативности обработки информации.

Из выражения (2.5) представленного выше следует, что время ОРС зависит от количества записей в хранилище. Но кроме данного аспекта на количественное значение ОРС влияют расположение хранилища в ИАС, пропускная способность каналов связи и структура организации информации в ИАС. Влияние последней характеристики может, как снижать, так и увеличивать значение ОРС.

Время, затраченное на регистрацию объекта, и время предобработки, как правило, являются результатом совместной работы модуля видеодетектирования и ЯИ. Если считать, что данные элементы в рамках всего класса, рассматриваемых ИАС, имеют одинаковые характеристики, а изменяется только тип обработки информации после получения шаблона, то можно сделать такой вывод. Следует принять за некоторую константу по отношению к $T_{соб}$ сумму времени регистрации объекта и предобработки. Кроме того будем считать, что $C_{соб}$ – характеристика ИАС, полученная в результате работы ряда одинаковых технических средств и алгоритмов, которая описывается формулой:

$$C_{\text{соб}} = (t_{\text{рег}} + t_{\text{ш}}). \quad (2.6)$$

Выражение (2.5) преобразуется следующим образом:

$$\text{Т}_{\text{соб}} = \frac{\text{С}_{\text{соб}} + t_{\text{выб}}}{\text{С}_{\text{соб}} + m * t_{\text{выб}}}. \quad (2.7)$$

Далее детально рассмотрим время $t_{\text{выб}}$:

$$t_{\text{выб}} = t_{\text{кс}} + t_{\text{х}} + t_{\text{стр}}, \quad (2.8)$$

где

- $t_{\text{кс}}$ – время, затраченное на передачу шаблона по всем возможным каналам связи, которые в своей работе использует ИАС (оно не велико, если хранилище расположено на одном сервере с ядром идентификации и модулями видеодетектирования, что распространенно в системах контроля управления доступом);
- $t_{\text{х}}$ – время, затраченное ИАС на получение информации по конкретному интересанту из хранилища с учетом реализации структуры данных;
- $t_{\text{стр}}$ – время обработки запроса с учетом структуры хранения информации.

Рассмотрим более подробно два последних элемента. Время $t_{\text{х}}$ характеризует качество работы конкретного программного средства в совокупности с вычислительными мощностями, используемыми в качестве сервера хранилища. В него входит время подготовки запроса на ЯИ (например, для БД – это *SQL* – Structure Query Language) и время выполнения данного запроса для конкретного хранилища (в ОП или БД). Это время зависит от количества записей в хранилище, будем полагать, что данная зависимость линейна, то есть

$$t_{\text{х}} = a_{\text{х}} * m + b_{\text{х}}, \quad (2.9)$$

где $a_{\text{х}}$ и $b_{\text{х}}$ – константы, характеризующие конкретное хранилище.

Рассмотрим время обработки запроса с учетом структуры хранения информации. Данная величина характеризует качество структуры хранения информации, например организацию таблиц и полей в БД. Время обработки запроса с учетом структуры хранения информации – также величина, зависящая от количества записей в хранилище. Данный вид зависимости требует отдельной

проработки, будем также полагать, что эта зависимость линейна. Кроме того, при определенных допущениях возможно включение параметра $t_{кс}$ в состав $t_{стр}$, тогда скорректированная формула (2.8) с учетом выражения (2.9) будет выглядеть следующим образом:

$$t_{выб} = a`_x * m + b`_x, \quad (2.10)$$

где $a`_x$ и $b`_x$ – константы, характеризующие конкретное хранилище, скорректированные с учетом использования в них данных о $t_{кс}$ и $t_{стр}$.

Далее формулу (2.7) можно записать в следующем виде:

$$T_{соб} = \frac{a'_x * m + b'_x + C_{соб}}{a'_x * m^2 + b'_x * m + C_{соб}}. \quad (2.11)$$

Подобрав соответствующим образом коэффициенты в уравнениях верхней и нижней части, упростим выражение (2.11). Пусть в общем случае решениями уравнения $a'_x * m^2 + b'_x * m + C_{соб}$ являются некоторые значения p и q. Тогда, исходя из правил решения квадратных уравнений, получается:

$$a'_x * m^2 + b'_x * m + C_{соб} = a'_x * (m + p) * (m + q). \quad (2.12)$$

После этого, учитывая, что

$$b`_x + C_{соб} = b"_x, \quad (2.13)$$

и установив соответствие:

$$a`_x * m + b"_x = Q_0, \quad (2.14)$$

где Q_0 – некоторая переменная, выражение $a'_x * m + b'_x + C_{соб}$ определим через некоторую величину, обозначенную как $Q_{соб}$:

$$a`_x * m + b"_x = (m + p) + Q_{соб}, \quad (2.15)$$

где (что следует из приравненных правых частей (2.14) и (2.15))

$$Q_{соб} = Q_0 * \left(1 - \frac{1}{a'_x}\right) + \frac{b''_x}{a'_x} - p. \quad (2.16)$$

Формулу (2.11) можно записать в следующем виде:

$$T_{соб} = \frac{m + p + Q_{соб}}{a'_x * (m + p) * (m + q)} \quad (2.17)$$

или

$$\mathrm{T}_{\text{соб}} = \frac{1}{a'_x*(m+q)} + \frac{Q_{\text{соб}}}{a'_x*(m+p)*(m+q)}. \quad (2.18)$$

Аналогичный вариант (2.18) может быть записан и с другим корнем уравнения (2.12), тогда (2.18) примет следующий вид:

$$\mathrm{T}_{\text{соб}} = \frac{1}{a'_x*(m+p)} + \frac{Q_{\text{соб}}}{a'_x*(m+p)*(m+q)}. \quad (2.19)$$

Данный вариант не рассматривается в исследовании в связи с аналогичностью с первым.

Из выражения (2.11), а также из формул (2.17) и (2.18) следует, что ОРС обратно пропорционально зависит от квадрата числа записей в хранилище. Для условности введем следующие обозначения:

$$A_{\text{соб}} = \frac{1}{a'_x*(m+q)}, \quad (2.20)$$

$$B_{\text{соб}} = \frac{Q_{\text{соб}}}{a'_x*(m+p)*(m+q)}. \quad (2.21)$$

Рассмотрим графики $T_{\text{соб}}$, $A_{\text{соб}}$ и $B_{\text{соб}}$ в двумерных прямоугольных декартовых координатах. При этом будем считать, что графики являются непрерывными, несмотря на дискретный характер числа записей в хранилище. И первая, и вторая составляющая в формуле (2.18) с математической точки зрения имеют «ветку графика», направленную в отрицательную сторону. Опустим отрицательные значения из рассмотрения.

На рисунке 2.2 приведена зависимость ОРС ($T_{\text{соб}}$) от количества записей в хранилище. Несмотря на то, что m принимает натуральные значения, графики зависимости $T_{\text{соб}}$ от m построены для действительных чисел. Данное допущение позволяет более полно анализировать результаты расчетов.

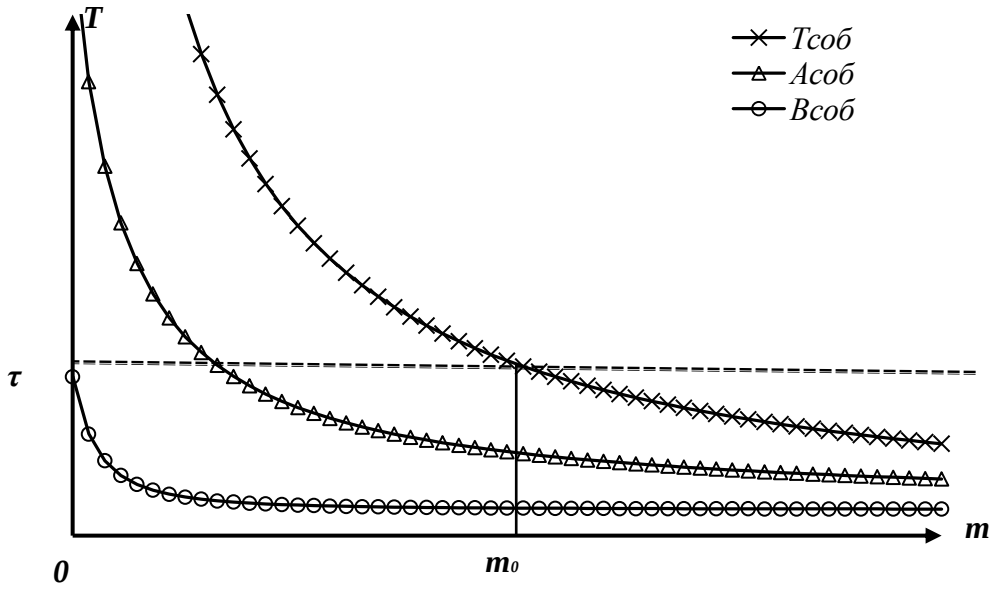


Рисунок 2.2. Зависимость ОРС от объема хранилища

Нулевое значение m соответствует пустому хранилищу. В этом случае обработка записи при получении запроса не выполняется. Пунктиром указан нижний порог эффективности (НПЭФ) ИАС. Будем полагать, что использование ИАС со значением ОРС ниже порога эффективности нецелесообразно. Таким образом, для эффективного функционирования ИАС должно выполняться следующее условие:

$$T_{\text{соб}} > \tau. \qquad (2.22)$$

Следовательно, необходимо, чтобы количество данных в хранилище не превышало некоторого значения m_0, т.е.

$$m < m_0 \ . \qquad (2.23)$$

Таким образом, объем данных в хранилище ИАС не должен превышать некоторого предельного значения, величина которого определяет эффективность взаимодействия ИАС с оператором. Далее эту величину (m_0) будем именовать верхним порогом числа записей (ВПЧЗ) хранилища. Предположим, что ИАС эффективно функционирует в режиме «реального времени», если идентификация человека осуществляется быстрее, чем за одну секунду. Следовательно, НПЭФ и ВПЧЗ необходимо выбирать на основании данного условия.

При этом, основываясь на статистических данных о работе ИАС с распознаванием лиц на небольших объектах, можно примерно оценить некоторый нижний порог количества записей в БД, исходя из устойчивости распознавания.

Надежность систем биометрической идентификации принято рассматривать в контексте вероятности следующих ошибок [62]:

1. Ошибки первого рода или false rejection rate. Данные ошибки отображает случаи, когда ИАС не распознает человека, информация о котором содержится в хранилище.
2. Ошибки второго рода или false acceptance rate. В случае, когда ИАС ложно идентифицирует человека и принимает его за другого, будем считать, что допущена ошибка второго рода.

Однако в случае применения в ИАС кластерной модели, а именно принципа «один кластер - один человек» [80], наиболее критичной является ошибка FAR, а не FRR. При функционировании ИАС на открытом множестве ошибка FRR приведет к созданию нового кластера, вследствие чего в результате поискового запроса будет представлена информация о нескольких кластерах. В случае же ошибки FAR кластер будет содержать информацию о разных людях. Данная ошибка отрицательно скажется как на точности распознавания, так и на достоверности результатов запросов оператора. Далее будем рассматривать зависимость надежности ИАС от объема хранилища в контексте вероятности ошибки 2-го рода.

Оценим нижний порог числа записей (НПЧЗ) в хранилище исходя из надежности распознавания. Для потока из n человек и хранилища, в котором содержится информация об m людях, вероятность возникновения ошибки второго рода (FAR_{mn}) можно рассчитать следующим образом:

$$FAR_{mn} = m * n * FAR. \quad (2.24)$$

Для надежного функционирования ИАС объем информации в хранилище должен быть заведомо выше потока людей ($m > n$). Тогда без ограничения

общности примем $n = m$. Допустив одну ошибку ложного совпадения на весь поток людей, можно получить оценку ошибки 2-го рода от объема хранилища:

$$m \approx \frac{1}{\sqrt{\mathrm{FAR}}}. \qquad (2.25)$$

Согласно рекомендациям Минстроя России по проектированию вокзалов пропускная способность среднего железнодорожного вокзала составляет от 200 до 700 пассажиров в час [37]. Из анализа графика зависимости значения ошибки 2-го рода от объема человеческого потока на среднем вокзале (рисунок 2.3) следует, что в местах массового скопления людей можно не учитывать НПЧЗ. Это объясняется тем, что даже при нижней границе человеческого потока (2.200 человек/час) вероятность ошибки 2-го рода составляет $2{,}5*10^{-5}$, а при достижении верхней границы (2.700 человек/час) уменьшается до $2*10^{-6}$. Таким образом, будем считать, что в местах массового скопления людей условие НПЧЗ всегда выполняется.

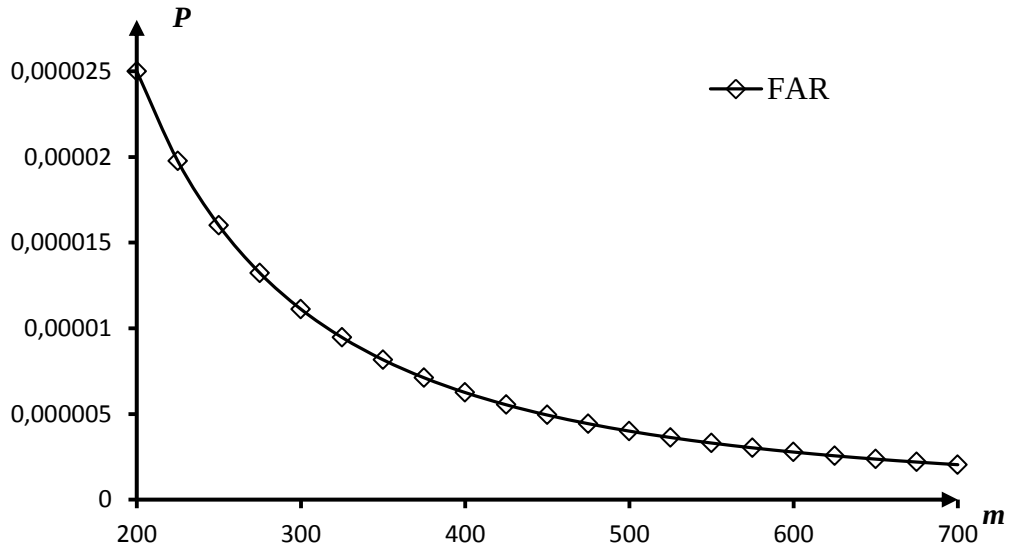


Рисунок 2.3. Зависимость FAR от объема хранилища

Таким образом, из приводимых расчетов и графиков следует, что для эффективной работы ИАС с возможностью распознавания лиц необходимо делить общий массив информации о лицах на части (кластеры). Данные кластеры должны составлять такую величину, которая позволит иметь необходимый объем информации для распознавания лиц, но количество кластеров должно позволять проводить распознавание за приемлемое время. Кроме того, увеличение скорости распознавания может быть достигнуто за счет использования распределенных

хранилищ различного типа. Следовательно, эффективной является ИАС, в которой не превышен ВПЧЗ. В данных предпосылках для работы ИАС в режиме «реального времени» предлагается использование распределенных хранилищ различного типа с применением кластеризации изображений по принципу: «один человек – один кластер». Основной целью предлагаемого решения является минимизация количества запросов к хранилищу на распознавание человека и повышение скорости распознавания. В силу высокой стоимости и ограниченности объема ОП, предлагается ее использовать для хранения лимитированного набора изображений одного человека, которые наиболее полно и качественно его представляют (центры кластеров), а БД – для долгосрочного хранения информации. Таким образом, при поступлении изображения лица человека с модулей видеодетектирования, будет достаточно сравнить его шаблон лица с шаблонами центров кластеров, хранимых в ОП. Теоретическая модель показывает, что данное ограничение объемов поиска сократит количество вычислительных операций и увеличит скорость и надежность реакции системы обеспечения безопасности.

2.3 Влияние сети видеоконтроля на систему поддержки управления

В процессе функционирования крупная ИАС, особенно при обеспечении массовых мероприятий, использует большое число источников данных. В рамках работы в качестве источников данных рассматриваются видеокамеры. В этих условиях оператору необходимо анализировать большое количество видеоматериала. Используя современные системы, например «Каскад-поток», оператор часто вынужден вручную отдавать команды системе на принудительное распознавание.

Выстроим математическую модель работы ИАС, в которой будет видна зависимость скорости реакции ИАС с оператором от числа и расположения камер, а также параметров регистрируемой информации. Будем строить модель, исходя из информации, используемой в существующих и используемых на сегодняшний день алгоритмах.

ЯИ и МД содержат программный код, основанный на наборе алгоритмов:

$$A_{соб} = \{A_1, A_2, \dots, A_p\} \quad (2.26),$$

где p – число алгоритмов, используемых в МД и ЯИ ИАС. Определим время ($t_{обр}$), затраченное на выполнение данных алгоритмов для распознавания одного человека и сопоставление с одним изображением лица:

$$t^1_{обр} = F(A_{соб}) + t_0, \quad (2.27)$$

где

- F – функционал на множестве алгоритмов распознавания $A_{соб}$;
- t_0 – некий начальный отрезок времени, не связанный с обработкой изображения и необходимый для его захвата и получения в нужном для обработки алгоритмом виде и одинаковый для всех камер.

Будем считать, что функционал F на наборе алгоритмов $A_{соб}$ обладает свойством аддитивности, тогда

$$t^1_{обр} = \sum_{i=0}^{p} F(A_i) + t_0, \quad (2.28)$$

где

$$A_i \in R^n, F(A_i) \to R. \quad (2.29)$$

Ряд алгоритмов, применяемых в ИАС, используются в ЯИ, а ряд в МД. Исходя из этого, уместно записать

$$A_{соб} = \{A_{яи} \mid A_{мд}\}, \quad (2.30)$$

где

- $A_{яи}$ – множество алгоритмов, применяемых в ЯИ;
- $A_{мд}$ – множество алгоритмов, применяемых в МД,

тогда справедливо следующее выражение:

$$t^1_{обр} = F(A_{яи} \mid A_{мд}) + t_0 \quad (2.31)$$

или

$$t^1_{обр} = F(A_{яи}) + F(A_{мд}) + t_0. \quad (2.32)$$

Если изображение лица интересанта сопоставляется с m изображения-ми, хранимыми в БД, то время обработки выражается следующим образом:

$$t^{m}_{\text{обр}} = m * F(A_{\text{яи}}) + F(A_{\text{мд}}) + t_0. \quad (2.33)$$

Заметим, что формула (2.33) согласуется с ранее полученным выражением (2.2).

Далее будем считать, что в один момент времени с одной камеры поступает одно изображение лица, тогда распознавание изображений лиц, поступающих из сети, состоящей из k видеокамер, можно выразить следующим образом:

$$t^{m}_{k} = k * (m * F(A_{\text{яи}}) + F(A_{\text{мд}})) + t_0. \quad (2.34)$$

Для t_0 следует заметить, что это в общем случае случайная величина, тогда в выражении (2.34) можно использовать формулу математического ожидания:

$$t_0 = M[T_0] = \int_0^{+\infty} t_0 * dF(t_0), \quad (2.35)$$

где $F(t_0)$ – функция распределения случайной величины.

Для простоты будем оценивать t_0 как

$$t_0 = \frac{1}{2}(t_0^{\text{ниж}} + t_0^{\text{врх}}), \quad (2.36)$$

где $t_0^{\text{ниж}}$ и $t_0^{\text{врх}}$ – статистически рассчитанные нижний и верхний пределы для отрезка времени t_0.

В формуле (2.34) сформулирована зависимость характеристики ИАС с распознаванием лиц от числа видеокамер и объема хранилища.

На основании формулы (2.34) можно получить асимптотическую временную сложность работы ИАС ($f(k,m)$) с возможностью распознавания человека на основе уникальности биометрии лица:

$$f(k,m) = O(k * (m + 1)), \quad (2.37)$$

где

- m – количество изображений лиц интересантов в хранилище;
- k – число камер в сети видеоконтроля.

Однако выражение (2.37) представляет худший случай, т.е. когда изображения лиц поступают со всех камер в сети видеоконтроля, а изображения в хранилище не отсортированы, и сравнение осуществляется в произвольном порядке.

Оценим среднее время работы ИАС ($g(k,m)$), т.е. математическое ожидание времени работы ИАС.

Распознавание интересанта представляется элементарным событием ω_j, где j является идентификационным номером личности, изображение которого содержится в хранилище ($j \in \{1 \dots m\}$). Множество элементарных событий образуют пространство элементарных событий $\Omega = \{\omega_1 \dots \omega_m\}$. В нашем случае алгебра событий A совпадает с множеством элементарных событий, т.е. $A = \Omega$. Так как сравнение изображения распознаваемого интересанта происходит со случайно выбранным изображением из хранилища, то будем считать, что элементарные события равновероятны, т.е. $\forall \omega_j \in \{\omega_1 \dots \omega_m\}$ ::

$$P(\omega_j) = \frac{1}{m}. \quad (2.38)$$

Таким образом, на вероятностном пространстве $(\Omega, A, P(\cdot))$ зададим случайную величину ζ как число необходимых сравнений для поиска личности в хранилище.

Можно показать, что случайная величина ζ является дискретной случайной величиной, равномерно распределенной на множестве $\{1 \dots m\}$. Тогда математическое ожидание случайной величины ζ, будет выражаться следующим образом [13]:

$$M[\zeta] = \sum_{i=1}^{m} x_i * p_i, \quad (2.39)$$

где

$$\zeta(\omega_i) = x_i \text{ и } P(\zeta(\omega_i) = x_i) = p_i. \quad (2.40)$$

Тогда путем преобразований (2.40) можно получить следующее значение математического ожидания:

$$M[\zeta] = \frac{m+1}{2}. \quad (2.41)$$

Математическое ожидание (2.41) отражает среднюю вычислительную сложность работы ИАС при распознавании одного интересанта. Вычислительная сложность обработки видеопотока с k камер выражается следующим образом:

$$g(k, m) = O\left(k * \left(\frac{m+1}{2}\right)\right). \quad (2.42)$$

Таким образом, если изображения в хранилище не отсортированы, и сравнение осуществляется в произвольном порядке, средняя сложность имеет вид выражения (2.42).

Но в случае наличия хранилища, содержащего достаточно большое количество изображений интересантов, основной составляющей времени распознавания является время, затраченное на запрос и получение информации о изображении лица из хранилища и сравнение с ним [81].

Далее повысим эффективность работы ИАС путем уменьшения количества операций сравнений. Повышение эффективности ИАС, а именно улучшение скорости реагирования, предлагается достигать за счет распараллеливания вычислений и уменьшения количества операций сравнения. Предлагается выделять группы камер, внутри которых обработка будет происходить последовательно, а вне группы – гарантированно параллельно. При этом время распознавания в группе будет иметь ту же линейную зависимость. А для всей ИАС время оно распознавания будет определяться временем распознавания в группе, в котором максимально:

$$t_k^m = \max_i t(i), \tag{2.43}$$

где

$$t(i) = r_i * (l_i * F(A_{яи}) + F(A_{мд})) + t_0 \text{ и } r_i < k,\ l_i < m \tag{2.44}$$

и

- i – индекс группы;
- l_i – количество анализируемых из хранилища изображений лиц интересантов в i-й группе;
- r_i – число камер в i-й группе сети видеоконтроля.

Таким образом, для эффективной работы ИАС должна быть настроена так, чтобы

$$r_i * (l_i * F(A_{яи}) + F(A_{мд})) + t_0 \rightarrow \min. \tag{2.45}$$

При этом необходимо, чтобы соблюдался ряд дополнительных условий. Проведем анализ ошибок первого и второго рода при работе ИАС. Оценим, как часто будут возникать пропуски и ложные совпадения [79].

Пусть система идентификации установлена на пункт контроля. Вероятность пропуска лица из хранилища равна FRR. Если принять допустимой одну ошибку пропуска интересанта при использовании информации о l_i людях, которые анализируются в блоке видеокамер, то

$$\mathrm{FRR} * l_i = 1. \quad (2.46)$$

Выразим l_i

$$l_i = \frac{1}{\mathrm{FRR}}. \quad (2.47)$$

Вероятность возникновения ошибки ложного совпадения для одного человека равна p^0_{fls}:

$$p^0_{\mathrm{fls}} = \mathrm{FAR} * l_i. \quad (2.48)$$

А вероятность возникновения ошибки ложного совпадения для потока изображений с r_i видеокамер равна p^1_{fls}:

$$p^1_{\mathrm{fls}} = \mathrm{FAR} * r_i * l_i. \quad (2.49)$$

Если принять допустимой одну ошибку ложного совпадения, то число ложных совпадений можно вычислять по формуле:

$$l_i = \frac{1}{(\mathrm{FAR} * r_i)} \quad (2.50)$$

или с учетом (2.45)

$$l_i = \frac{\mathrm{FRR}}{\mathrm{FAR}}. \quad (2.51)$$

Этот набор условий позволяет определять эффективность распознавания внутри группы видеокамер с учетом появления ложных срабатываний.

Другой набор условий может определять количество камер, которые необходимо привлекать к поиску интересанта. В общем случае, когда входные условия поиска всегда одинаковые, то для поиска и регистрации привлекаются все камеры и все кластеры. В этом случае (2.34) имеет максимальное значение.

Теперь предположим, что выбор камер, которые будут использоваться для идентификации интересанта, зависит от группы из h условий:

$$G = \{g_1, g_2, \ldots, g_h\}, \quad (2.52)$$

тогда количество камер в блоке

$$r_{i0} = \varphi^i(G) \quad (2.53)$$

и при этом

$$r_{i0} \leq r_i. \quad (2.54)$$

С математической точки зрения это означает, что в (2.45) параметр r_i будет уменьшаться, и, следовательно, будет уменьшаться и искомое значение t_k^m.

Если ввести параметры нумерации камер и кластеров ИАС, то в качестве условий (2.52) можно задавать номера камер следующим образом:

- с привязкой к предварительной информации о местах пребывания интересантов;

- с привязкой к «следам» их пребывания на основе анализа видеоданных из камер на интересанта за предыдущие периоды работы ИАС;

- с привязкой к местам, где они чаще всего появляются, с заданием частоты появления в качестве весового коэффициента для вершины графа.

Тогда, решая задачу (2.45) одним из известных методов обхода графа, можно в разы сократить параметр t_k^m, отражающий суммарное время работы распознающей части и существенно снизить нагрузку на вычислительные средства обрабатывающего центра ИАС.

Далее в качестве условий объединения камер в группы рассмотрим задание возможных мест появления физических лиц. Данную кластеризацию можно осуществить следующими способами:

a. Отслеживание движения. При попадании физического лица в объектив камеры, распознавать его, а затем отслеживать его передвижение. Но почти у всех методов отслеживания движения присутствуют недостатки: принятие элементов фона в качестве движущихся объектов, низкая производительность системы трекинга, многочисленные ошибки при перекрытие объектов, игнорирование объектов при их малом размере или малой амплитуде движения и т. д.

b. Построение вероятностного графа маршрутов (рисунок 2.4). Сеть видеоконтроля с установленными в разных местах видеокамерами можно условно рассматривать в качестве нагруженного графа, ребра которого несут определенную нагрузку. В качестве такой нагрузки будем рассматривать значение вероятности (q_{ij}) того, что интересант пришел в конечную вершину (j) из начальной (i). Следовательно, рассмотрим ориентированный граф возможных маршрутов передвижения интересанта. Вершинами графа являются места видеофиксации (вход, касса и прочее). Каждое ребро графа помечено меткой, значение которой является вероятностью того, что интересант в предыдущий момент времени

находился в вершине (i), при условии, что сейчас он находится в вершине (j).

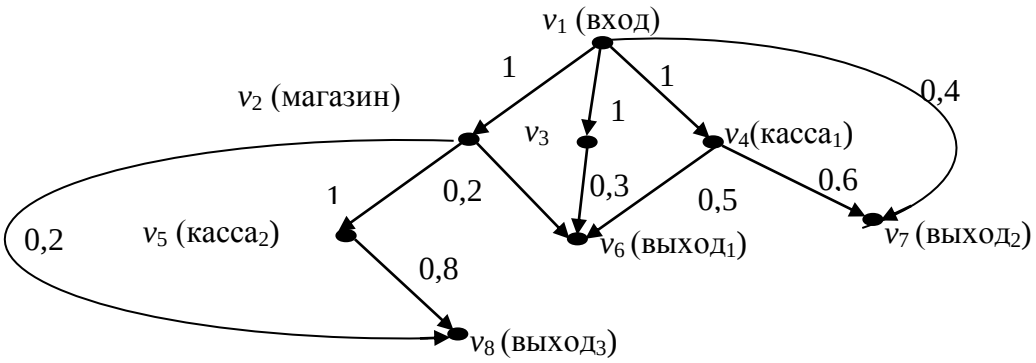


Рисунок 2.4. Пример вероятностного графа маршрутов

Для построения графа вероятностных маршрутов можно воспользоваться теорией случайных процессов в части, касающейся конечных однородных Марковских цепей.

Рассмотрим следующий случайный процесс на фазовом пространстве E

$$\{\xi_n, n \in N\}, \tag{2.55}$$

где

- ξ_n – случайная величина, равная идентификатору камеры, которая зафиксировала интересанта;
- n – порядковый номер камеры, которая зафиксировала интересанта (момент времени);
- $E = \{1 \ldots m\}$ – фазовое пространство. Элементами данного множества являются идентификаторы камер.

Проверим, что случайный процесс, описанный в выражении (2.55) является конечной однородной Марковской цепью (далее – КОМЦ):

1) Данный процесс является цепью, поскольку временное пространство $T = N$ – дискретно.
2) Будем считать, что цепь, описанная в выражении (2.55) обладает Марковским свойством, т.е. $\forall n \in N, \forall i, j, i_{n-1}, \ldots i_0 \in E$ верно равенство:

$$P\{\xi_{n+1} = j \mid \xi_n = i, \xi_{n-1} = i_{n-1} \dots, \xi_n = i_0\} = P\{\xi_{n+1} = j \mid \xi_n = i\} \quad (2.56)$$

Данное допущение вполне уместно, так как то в поле видимости, какой камеры окажется интересант в момент времени $n + 1$, зависит только от того, где он был в момент времени n.

3) Конечность Марковской цепи следует из того, что мощность фазового пространства E равна m.
4) Будем считать, что условные вероятности $P\{\xi_{n+1} = j \mid \xi_n = i\}$ не зависят от n, т.е. $\forall n \in N, \forall i, j \in E$:

$$P\{\xi_{n+1} = j \mid \xi_n = i\} = \dots = P\{\xi_1 = j \mid \xi_0 = i\}. \quad (2.57)$$

Тогда случайный процесс, описанный в выражении (30) является однородным.

Далее на основе статистической информации необходимо задать матрицу переходных вероятностей:

$$\Pi = \begin{pmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mm} \end{pmatrix}, \quad (2.58)$$

где p_{ij} – вероятность того, что интересант будет находиться в поле видимости камеры с идентификаторам j при условии, что до этого он находился в поле видимости камеры с идентификаторам i.

Тогда метки ребер q_{ij} вероятностного графа маршрутов могут быть получены следующим образом:

$$q_{ij} = P\{\xi_n = i \mid \xi_{n+1} = j\} = \frac{P\{\xi_n = i\} * P\{\xi_{n+1} = j \mid \xi_n = i\}}{P\{\xi_{n+1} = j\}}. \quad (2.59)$$

Описанная выше выкладка позволяет произвести распознавание интересанта следующим образом: при распознавании интересанта в узле сети видеоконтроля необходимо сравнивать лицо с уже идентифицированными лицами в смежных вершинах в порядке уменьшения значения метки ребра (например, при идентификации в узле v_6 необходимо сравнивать сначала изображения, зафиксированные в узле v_4, далее если соответствие не установлено, то и в v_3 и v_2).

Далее из свойств КОМЦ следует [28], что фазовое пространство $E = \{1 \ldots m\}$ разбивается в объединение не пересекающихся классов взаимно сообщающихся состояний:

$$E = E_1 \sqcup \ldots \sqcup E_{n_1} \sqcup \{j_1\} \sqcup \ldots \sqcup \{j_{n_2}\}, \quad (2.60)$$

где:

- $E_1, \ldots, E_{n_1}$ – не пересекающиеся классы взаимно сообщающихся существенных не поглощающих состояний;
- $\{j_1\}, \ldots, \{j_{n_2}\}$ – существенные поглощающие состояния.

Таким образом, множество идентификаторов камер распадается на не пересекающиеся классы. При распознавании интересантов в разных группах осуществляется обращение к разным исходным данным. В результате применения параллельной обработки данных между группами будет увеличено быстродействие ИАС в целом.

Далее остановимся на оценке точности и вычислительной сложности распознавания интересанта при использовании вероятностного графа маршрута.

Например, если принять, что вероятность ошибки распознавания при сравнении изображения с хранилищем, содержащим информацию об m интересантах, выражается следующим образом:

$$q_1 = P(m), \quad (2.61)$$

а вероятность ошибки распознавания при сравнении изображения с кадрами из предыдущего узла:

$$q_2 = P(m_0), \quad (2.62)$$

где m_0 – число изображений в предыдущем узле, тогда, если

$$m_0 << m, \quad (2.63)$$

и в предыдущем узле распознавание произошло правильно, можно показать

$$q_2 > q_1. \quad (2.64)$$

А также вычислительная сложность распознавания ИАС тоже уменьшится и составит:

$$f(k,m) = O(r * \left(\frac{l+1}{2}\right)), \quad (2.65)$$

где $l << m$ и $r << k$. Следовательно, с применением вероятностного графа маршрутов точность и время распознавания улучшились.

Таким образом, анализ ИАС показал возможность создания модели работы алгоритмов ИАС при распознавании лиц с нагрузкой от сети видеоконтроля. Анализ условий возможного применения модели показал наличие ряда характеристик, фиксируемых и определяемых совместно с распознаванием, которые позволяют существенно уменьшить суммарное время обработки данных и улучшить точность распознавания. Это возможно обеспечить за счет привязки к номеру камеры данных о местах и частотах пребывания интересантов в определенных местах в определенный период. Кроме того, применение конечных однородных Марковских цепей к сети видеоконтроля позволило разбить множество камер в объединение не пересекающихся групп, внутри которых ИАС может обрабатывать информацию об интересантах последовательно, а вне групп – параллельно.

2.4 Методы кластерного анализа в системе поддержки управления

При распознавании лиц в ИАС существуют проблемы, связанные со старением информации. Так, например, в [23] приводятся данные анализа различных алгоритмов, который проводился в рамках американской программы FERET. В тестах этой программы несколько лет подряд проверялись алгоритмы гибкого сравнения на графах и модификации метода главных компонент. «Эффективность всех алгоритмов была примерно одинаковой. В этой связи трудно или даже невозможно провести четкие различия между ними (особенно если согласовать даты тестирования). Для фронтальных изображений, сделанных в один и тот же день, приемлемая точность распознавания, как правило, составляет 95%. Для изображений, сделанных разными аппаратами и при разном освещении, точность, как правило, падает до 80%. Для изображений, сделанных с разницей в год, точность распознавания составило примерно 50%».

Для функционирования ИАС в режиме реального времени зачастую такие результаты могут быть недостаточными. Поэтому необходимо иметь предложения по повышению эффективности распознавания и уменьшению времени на распознавания. Не секрет, что фронтальное изображение имеет наилучшие характеристики в распознавании. И фотографии, используемые в ИАС в качестве шаблонов лиц интересантов, обычно имеют этот же ракурс. Тем не менее, реальных условиях лица обычно повёрнуты относительно этого положения. Поэтому лица принято объединять в кластеры. Один из примеров из [23] изображён на рисунке 2.5.

Рисунок 2.5 Пример кластера лица человека

Для работы с такими наборами информации принято использовать кластерный анализ. В [10] эта предметная область определена так: «кластерный анализ (самообучение, обучение без учителя, таксономия) применяется при автоматическом формировании перечня образов по обучающей выборке. Все объекты этой выборки предъявляются системе без указания, какому образу они принадлежат… Предполагается, что обучающая выборка в признаковом пространстве состоит из набора сгустков (подобно галактикам во Вселенной). Задача системы – выявить и формализовано описать эти сгустки» (с.23). Такая точная цитата как раз соответствует набору изображений на рисунке 2.5. Эти

«сгустки» принято также называть таксонами. Но в технической литературе, относящейся не к математическим построениям, а к распознаванию видео, обычно используется термин кластер.

Однако, как в кластерном анализе, так и в распознавании видео главный вопрос заключается в том, как отнести входной объект к нужному таксону (кластеру). Для этого используют понятие «близости» или расстояния. Но так как в многомерном объекте характеристик достаточно много, то и математических понятий для него тоже много. Для разных задач кластерного анализа в технической литературе предложен ряд методов классификации.

Задача такого анализа строится на определении некоторой метрики или функции, позволяющей соотнести новый объект с уже имеющимися. Для этого каждый из содержащихся в множестве объектов имеет своё значение данной метрики. А правила классификации позволяют соотнести это значение с тем или иным классом (кластером, таксоном). В идеальном варианте всё множество объектов Z разбивается на ряд таксонов или кластеров так, что

$$Z = \{Z_1, Z_2, \ldots, Z_m\}, \qquad Z_1 \cap Z_2 \cap \ldots \cap Z_m = \emptyset, \tag{2.66}$$

Зачастую такое разбиение сложно получить, тогда множество Z стремятся разбить следующим образом:

$$Z = \{Z_1, Z_2, \ldots, Z_m\}, \qquad Z_1 \cap Z_2 \cap \ldots \cap Z_m \neq \emptyset \tag{2.67}$$

и при этом

$$\exists\, Z` \in Z,\ Z` = \{Z`_1, Z`_2, \ldots, Z`_m\},\ Z`_1 \cap Z`_2 \cap \ldots \cap Z`_m = \emptyset. \tag{2.68}$$

Иными словами, внутри кластеров множества Z существуют такие подмножества $Z`$, которые никогда не пересекаются.

Тогда ([35], п.3.4) могут быть определены некоторые функции:

$$F = \{R^n \rightarrow R^1\} \tag{2.69}$$

на основании, которых можно будет различать между собой $Z`_1, Z`_2, \ldots, Z`_m$. При этом

$$F = \{f_1, f_2, \ldots, f_m\}. \tag{2.70}$$

Здесь f_1, f_2, …, f_m – функции для каждого из кластеров. Они определяются на пространстве признаков размерностью n. И для них в простейшем случае должно выполняться такое условие:

$$f_i(X) > 0, \forall X \in Z`_i, \quad (2.71)$$

где X – набор признаков классифицируемого объекта.

В более сложном случае функции (2.69) представляют собой расстояния между объектами. В этом случае по признакам объекта X и какого-то представителя таксона $Z`_i$, который вычисляется в соответствии с требованиями модели классификации и хранения, по заданным правилам вычисляется метрика:

$$f_i(X) \leq \tau, \forall X \in Z`_i, \quad (2.72)$$

где τ – некоторая характеристика (порог) качества распознавания.

Сравнение значения функции (функционала) $f_i(X)$ с заданным порогом τ определяет качество распознавания в системе. При этом обычно полагается, что $\tau \in R^1$.

Важным обстоятельством является то, что признаки объектов X являются результатом определённых наблюдений и преобразований. Поэтому признаки являются значениями, регистрируемыми при помощи датчиков:

$$X = \{ d_1(X), d_2(X) \ldots, d_r(X) \}, \quad (2.73)$$

где $d_i(X)$ – показания r датчиков, при этом зачастую

$$d_i(X) = \{R^n \rightarrow R^1\}. \quad (2.74)$$

Но есть и другие способы получения данных о признаках. В статье [38] эти способы определены так: «Качество решающего правила измеряют частотой появления правильных решений. Обычно его оценивают, наделяя множество объектов W некоторой вероятностной мерой. Тогда задача записывается в виде»

$$\min P(\hat{g}(x(w)) \neq g(w)), \quad (2.75)$$

где

- w – образ из пространства образов $\hat{W}$, $w \in \hat{W}$;
- $x(w)$ – функция, ставящая в соответствие каждому объекту w точку x(w) в пространстве признаков или образ объекта, определяемый наблюдателем;

- $\hat{g}(w)$ – решающее правило, определяющее попадает ли объект с комбинацией признаков x в пространство кластеров;
- $g(w)$ – оценка функции $\hat{g}(w)$;
- $P(\cdot)$ – вероятностная мера, определяющая неравенство значений функции решающего правила и её оценки.

Принадлежность объекта к одному из классов всегда определяется с помощью расстояний между ним и всеми объектами, соответствующими эталонным образам в классах распознавания. Оно является мерой его сходства с эталонами классов или образов. Функции (2.69) – это обобщённое расстояние.

Для измерения значений функций (2.69) применяют разные формулы. В зависимости от различных условий решения задач об автоматической классификации объектов с помощью кластерного анализа. Рассмотрим ряд методов определения расстояния. Для иллюстрации этого воспользуемся источником [44]. В нём даны следующие определения.

«Метрики – важный инструмент решения многих задач распознавания образов и интеллектуального анализа данных. Наличие метрики в пространстве позволяет принимать решение о принадлежности к множеству или о сходстве множеств на основе количественного показателя …

Метрика – функция, которая каждой упорядоченной паре точек x и y пространства, ставит в соответствие, действительное число $d(x, y)$ …

Введение метрики $d(x, y)$ в пространстве изображений позволяет говорить о близости или удаленности точек в этом пространстве или о мере сходства или различия анализируемых изображений» (с.13).

Пространства, в которых определена метрика, называются метрическими. В них каждая из точек определена как вектор. Тогда, если входное и хранимое изображения есть набор признаков, то каждый из этих признаков может быть вектором. Следовательно, между ними можно найти расстояние. Соответственно, сам кластер задаётся как группа векторов или матрица.

Матрица менее удобный с точки зрения простоты вычислений математический инструмент, чем вектор. Поэтому, ввиду возможной её большой размерности, для сокращения размерности и меньших затрат на хранение были предложены варианты обработки изображений, связанные с вычислением собственных векторов.

Конкретные формулы для вычисления расстояния рассмотрим ниже. Примем расстояние между двумя объектами в виде $d(x, y)$, где x – новый объект, для которого вычисляется расстояние, а y – объект в хранилище, и при этом выполняется следующее:

$$y \in Z` = \{Z`_1, Z`_2, \ldots, Z`_m\},\ Z`_1 \cap Z`_2 \cap \ldots \cap Z`_m = \emptyset, \qquad (2.76)$$

где m – число кластеров, записанных в виде математических объектов в хранилище.

При этом общее число записей в хранилище составляет N. Тогда под единичным вычислением $s(d_i)$ будем понимать набор операций по вычислению i-того признака в метрике $d(x, y)$, где $x \in X$, которое определяется в (2.70), а $y \in Y = \{Y_1, Y_2, \ldots, Y_l\}$, где $l = m * r$ и r – число признаков по которым осуществляется сравнение. Число операций сравнения, необходимое для вычисления $d(x, y)$, выражается следующим образом:

$$S(x, y) = \sum_r s(d_i). \qquad (2.77)$$

Тогда для сравнения с m элементами Y необходимо

$$S^+(x, y) = \sum_m \sum_r s(d_i). \qquad (2.78)$$

Соответственно для N записей в хранилище

$$S^N(x, y) = \sum_N S^+(x, y). \qquad (2.79)$$

Тогда модель применения методов кластерного анализа в ИАС к распознаванию лиц может быть записана в виде:

$$S^N(x, y) \to min. \qquad (2.80)$$

Очевидно, что в этом случае частота сравнений при поиске имеет определяющее значение.

Таким образом, для сокращения количества вычислений при применении методов кластерного анализа в ИАС к распознаванию лиц целесообразно максимально сократить количество сравнений в процессе функционирования.

Сокращение количества сравнений может быть достигнуто за счет кластеризации изображений: «один человек – один кластер». Тогда новое анализируемое изображение достаточно будет сравнивать не со всеми изображениями в хранилище, а с одним изображением из кластера.

Выбор изображений из каждого кластера для сравнения необходимо осуществлять, основываясь на освещённости, масштабе и ракурсе наблюдения в анализируемом изображении. Данное требование обусловлено тем, что большинство алгоритмов распознавания лиц разработаны для изображений с примерно одинаковым ракурсом лиц, масштабом и уровнем освещённости и демонстрируют некорректные результаты при большом отличии в данных параметрах.

Одним из перспективных направлений является проведение расчётов по поиску наиболее подходящего изображения каждого из кластеров не в момент поступления нового изображения, а в тот момент, когда ИАС не «занята». Такой момент может наступить во время визуальной обработки данных оператором, либо по окончании выдачи данных из хранилищ. Кроме того, исходя из (2.78) уместно предположить, что хранение наиболее подходящих изображений в поисковых кластерах отдельно от остальных изображений в разы сократит количество вычислительных операций.

2.5 Управление мероприятиями мониторинга и противодействия дестабилизациям

На сегодняшний день не существует нормативно-правовых документов и стандартов, определяющих эффективность систем класса рассматриваемой ИАС. Однако существуют стандарты в смежных областях, например ГОСТ Р 50776-95 [21], для систем с охранной сигнализацией. Согласно стандарту, система должна обеспечивать защиту в соответствии с требуемым уровнем. Воспользуемся

данным определением при построении и разработке методики определения эффективности управления безопасностью в общественном месте, оборудованном ИАС. Под показателем эффективности будем понимать вероятность защиты объекта, а именно вероятность своевременного реагирования на пожар и интересанта.

Далее выстроим методику определения эффективности управления безопасностью в местах массового пребывания (общественных месте), оборудованного ИАС.

Воспользуемся подходом, описанным в статье [98], для оценки вероятности защиты объекта $P_{зо}$:

$$P_{зо} = P_{обн} * P_{бр} * P_{пр} * P_{н}, \quad (2.81)$$

где

- $P_{обн}$ – вероятность обнаружения вторжения;
- $P_{бр}$ – вероятность безотказной работы системы;
- $P_{пр}$ – вероятность перехвата нарушителей силами охраны на объекте;
- $P_{н}$ – вероятность нейтрализации интересанта силами охраны.

Однако в указанной статье полагалось, что система функционирует безотказно ($P_{бр} = 1$), осуществляется обнаружение проникновения нарушителя ($P_{обн} = 1$) и в случае прибытие группы реагирования происходит его нейтрализация ($P_{н} = 1$). Тогда вероятность защиты объекта определяется вероятностью того, что прибытие группы вневедомственной охраны к объекту произойдет раньше, чем нарушитель совершит противоправные действия и покинет объект (2.81).

$$P_{зо} = P_{пр} = 1 - P(t_{и} > t_{р}), \quad (2.82)$$

где:

- $t_{и}$ – интервал времени с начала проникновения нарушителя до совершения им деструктивного действия или покидания объекта;
- $t_{р}$ – время реагирования сил и средств вневедомственной охраны на возникшую тревожную ситуацию.

Данный подход можно использовать и для оценки эффективности управления безопасностью общественного места, оборудованного ИАС.

Вместе с тем имеющиеся оценки функционирования ИАС [33] не позволяют сделать вывод об их абсолютной надежности и моментальности обнаружения нарушителя. Следовательно, необходимо оценить скорость идентификации интересанта и время реагирования оператора ИАС при оценки защиты объекта.

Тогда провести оценку эффективности взаимодействия ИАС и оператора возможно на основе метода совместного реагирования. А именно необходимо построить функции оценки эффективности ИАС θ_1 (t) и оценки реагирования оператора θ_2 (t).

Рассмотрим случайную величину θ_1, равную времени реакции оператора ИАС на нарушителя. На основании исследований [85] будем считать, что функция реагирования оператора имеет вид:

$$\theta_1 = a_0 {x_1}^{l_0}(t) \dots {x_n}^{v_0}(t) + \cdots + a_{h-1} {x_1}^{l_{h-1}}(t) \dots {x_n}^{v_{h-1}}(t), \qquad (2.83)$$

где

- ${x_1}^{l_i}(t) \dots {x_n}^{v_i}(t)$ – показатели (факторы) эффективности сотрудника (объекта управления), которые являются независимыми переменными (внимательность, скорость реакции и т.д.);
- $a_0, \dots, a_{h-1}$ – коэффициенты регрессии, определяющиеся по результатам испытаний;
- h – количество испытаний.

На основе регрессионного анализа [58] (например, с использованием метода наименьших квадратов) можно выбирать управляющие воздействия, а именно менять показатели сотрудника, которые позволят повысить его эффективность взаимодействия с ИАС, а именно:

- прогнозировать состояние объекта управления при ожидаемых сочетаниях показателей эффективности сотрудника;
- формировать управляющие воздействия по подконтрольным показателям с целью поддержания (или изменения по требуемому закону) состояния объекта управления в заданной области фазового пространства управления;

- упорядочить показатели эффективности сотрудника по степени значимости их влияния на эффективность обеспечения безопасности;
- находить экстремум функции реагирования θ_1 на множестве показателей эффективности сотрудника для определения наиболее благоприятных или опасных их сочетаний.

Аналогично рассмотрим случайную величину θ_2, равную времени обнаружения нарушителя ИАС. На основании формулы (2.44) можно получить выражение для θ_2:

$$\theta_2\ (m(t), t_0, t_{\text{рег}}, t_{\text{ш}}, k(t)) = k *((t_{\text{рег}} + t_{\text{ш}} + (a`_{\text{х}} * m + b`_{\text{х}})* m) + t_{\text{дет}}) + t_0. \qquad (2.84)$$

Данная функция (2.83) и методы повышения эффективности ИАС детально рассмотрены в предыдущих разделах.

Случайным величинам θ_1 и θ_2 соответствует своя функция распределения:

$$F_{\theta_i}(t) = P\{\theta_i < t\}, \quad \forall t \in R, i \in \{1, 2\}. \qquad (2.85)$$

Будем считать, что случайные величины θ_1 и θ_2 независимы и имеют абсолютно непрерывное распределение, тогда существуют плотности $f_{\theta_i}(\,)$:

$$F_{\theta_i}(t) = \int_{-\infty}^{t} f_{\theta_i}(y)\, dy, \ i \in \{1, 2\}. \qquad (2.86)$$

Далее воспользуемся теоремой о свертки независимых и абсолютно непрерывных случайных величин [31]. Согласно данной теореме сумма случайных величин θ_1 и θ_2 образуют абсолютно непрерывную случайную величину с функцией распределения:

$$F_{\theta_1+\theta_2}(t) = \int_{-\infty}^{+\infty} F_{\theta_1}(t-\tau)\, f_{\theta_2}(\tau) d\tau, \ i \in \{1, 2\}. \qquad (2.87)$$

Таким образом вероятность того, что время реакции ИАС и оператора ИАС на нарушителя будет меньше времени покидания нарушителем пространства обзора видеокамеры:

$$P\{\theta_1 + \theta_2 < \Delta t_{\text{и}}\} = P\left\{\theta_1 + \theta_2 < \frac{\Delta x}{v}\right\} = F_{\theta_1+\theta_2}\left(\frac{\Delta x}{v}\right) = \\ = \int_{-\infty}^{+\infty} F_{\theta_1}\left(\frac{\Delta x}{v} - \tau\right) f_{\theta_2}(\tau) d\tau, \qquad (2.88)$$

где

- $\Delta t_{и}$ – время нахождения нарушителя в пространстве обзора видеокамеры;
- Δx – отрезок маршрута движения нарушителя, который попадает в обзор видеокамеры;
- v– скорость движения нарушителя.

Далее необходимо оценить вероятность обнаружения нарушителя при перемещении по траектории из точки A в точку B (рисунок 2.6). Для этого разделим траекторию движения на отрезки. Будем считать, что на данной траектории движения установлено множество видеокамер. При этом на одном отрезке маршрута его движения установлено не больше одной видеокамеры. Время обнаружения нарушителя при его попадании в поле видимости одной камеры определяется выражением (2.87).

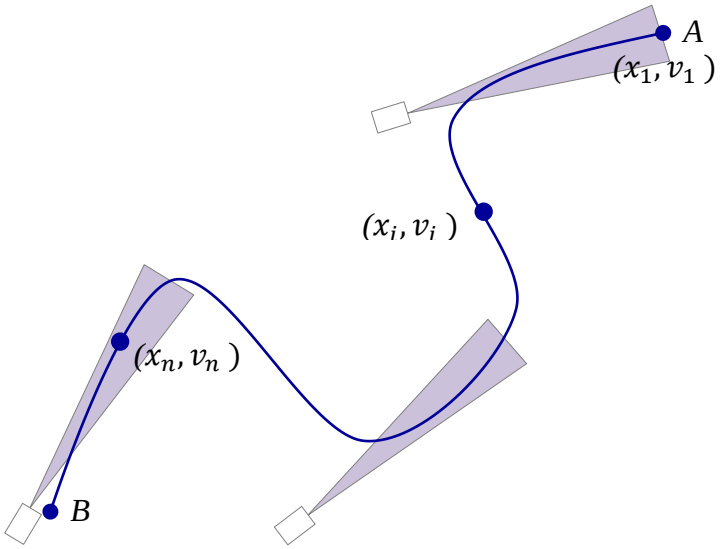


Рисунок 2.6. Траектория движения нарушителя

Построим вероятностное пространство $(\Omega,\ A, P(\ ))$:

- $w = (\varepsilon_1, \dots, \varepsilon_n)$ – элементарное событие, где $\varepsilon_i \in \{0,1\}$– исход попытки обнаружения нарушителя на i-ом отрезке маршрута;
- n – количество отрезков, на которые разделен маршрут;
- $\Omega = \{w\}$ – пространство элементарных событий;
- $A = \rho(\Omega) = 2^{\Omega}$ – класс событий;
- вероятностную функцию определим заданием вероятностей для всех элементарных событий: $P\ \ (\ \ ) = \{P\{\varepsilon_1, \dots, \varepsilon_n\} | \ \forall w = (\varepsilon_1, \dots, \varepsilon_n) \in \Omega\}$.

Рассмотрим событие $A_i^{\varepsilon_i}$= «на i-ом отрезке маршрута произошел исход ε_i». Оно определяется только результатом исхода попытки обнаружения нарушителя

на i-ом отрезке маршрута. Следовательно, $A_1^{\varepsilon_1} \dots A_n^{\varepsilon_n}$– независимые события и $w = (\varepsilon_1, \dots, \varepsilon_n) = A_1^{\varepsilon_1} \cap \dots \cap A_n^{\varepsilon_n}$, тогда:

$$P\{(\varepsilon_1, \dots, \varepsilon_n)\} = P(A_1^{\varepsilon_1}) * \dots * P(A_n^{\varepsilon_n}). \quad (2.89)$$

Будем считать, что нарушитель обнаружен, если он обнаружен хотя бы на одном отрезке маршрута передвижения, т.е.:

$$P_{\text{обн на } (A,B)} = 1 - P\{(0, \dots, 0)\} = \ 1 - P(A_1^0) * \dots * P(A_n^0) =$$
$$= 1 - \left(1 - F_{\theta_1+\theta_2}\left(\frac{\Delta x_1}{v}\right)\right) * \dots * \left(1 - F_{\theta_1+\theta_2}\left(\frac{\Delta x_1}{v}\right)\right) = 1 - \quad (2.90)$$
$$\prod_{\Delta x \epsilon (A,B)}\left(1 - F_{\theta_1+\theta_2}\left(\frac{\Delta x}{v}\right)\right).$$

Окончательное выражение для определения вероятности обнаружения нарушителя на маршруте следования из точки A в точку B:

$$P_{\text{обн на } (A,B)} = 1 - \prod_{\Delta x \epsilon (A,B)}\left(1 - \int_{-\infty}^{+\infty} F_{\theta_1}\left(\frac{\Delta x}{v} - \tau\right) f_{\theta_2}(\tau) d\tau\right), \quad (2.91)$$

где

- (A, B) –траектория движения нарушителя;
- v_i– скорость движения нарушителя на i-ом участке маршрута;
- $F_{\theta_1}(\ \ )$ – функция распределения случайной величины реакции оператора на нарушителя;
- $f_{\theta_2}(\ \ )$ – плотность случайной величины реакции ИАС на нарушителя.

Таким образом, будем считать, что эффективность ИАС – это минимум из всех вероятностей обнаружения нарушителя на множестве всех возможных траекториях его движения:

$$E = \min_{(A,B)}\left(1 - \prod_{\Delta x \epsilon (A,B)}\left(1 - \int_{-\infty}^{+\infty} F_{\theta_1}\left(\frac{\Delta x}{v} - \tau\right) f_{\theta_2}(\tau) d\tau\right)\right). \quad (2.92)$$

Согласно подходу, описанному в статье [98], временные случайные величины ИАС обладают нормальным законом распределения (рисунок 2.7). Тогда плотность будет определяться следующим образом:

$$f_{\theta_i}(t) = \begin{cases} 0, & \text{при } t \le 0 \\ \frac{1}{\sigma_{\theta_i} * \sqrt{2*\pi}} e^{\frac{-\left(t - M(\theta_i)\right)^2}{2 * \sigma_{\theta_i}^2}}, & \text{при } 0 < t < \infty \end{cases}, i \in \{1,2\}. \quad (2.93)$$

Воспользовавшись функцией Лапласа, получим:

$$F_{\theta_i}(t) = \Phi\left(\frac{t-M(\theta_i)}{\sigma_{\theta_i}}\right), i \in \{1,2\}, \quad (2.94)$$

где Ф – функция Лапласа.

Будем считать, что случайные величины θ_1, θ_2 независимы и имеют нормальное распределение. Тогда на основе работы [8]

$$F_{\theta_1+\theta_2}(t) = \Phi\left(\frac{t-(M(\theta_1)+M(\theta_2))}{\sqrt{\sigma^2\theta_1+\sigma^2\theta_2}}\right). \quad (2.95)$$

Далее преобразуем выражение (2.90) с использованием формулы (2.95):

$$P_{\text{обн на }(A,B)} = 1 - \prod_{\Delta x \epsilon (A,B)} \left(1 - \Phi\left(\frac{\frac{\Delta x}{v}-(M(\theta_1)+M(\theta_2))}{\sqrt{\sigma^2\theta_1+\sigma^2\theta_2}}\right)\right). \quad (2.96)$$

Таким образом, критерием эффективности управлением безопасности общественного места является достижение такого уровня $P_{\text{зо}}$, который будет превышать установленный порог защиты $P_{\text{зп}}$:

$$\min_{(A,B)}\left(1 - \prod_{\Delta x \epsilon (A,B)} \left(1 - \Phi\left(\frac{\frac{\Delta x}{v}-(M(\theta_1)+M(\theta_2))}{\sqrt{\sigma^2\theta_1+\sigma^2\theta_2}}\right)\right)\right) > P_{\text{зп}}. \quad (2.97)$$

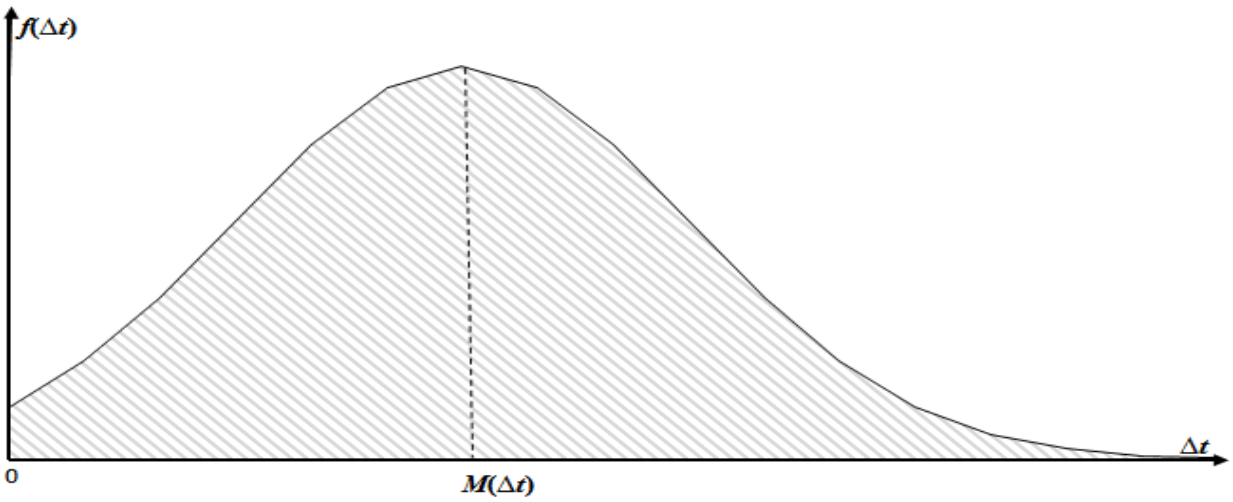


Рисунок 2.7 Оценка вероятности защиты объекта

После того как интересант обнаружен может возникнуть задача его задержания. Однако месту массового пребывания людей свойственна большая

площадь. Данное обстоятельство может существенно осложнить задержание. Попросту интересант может скрыться ни о чем, не подозревая в период с момента его обнаружения до прибытия сотрудников безопасности.

В связи с этим в данной работе предлагается подход, с использованием которого орган управления, может обоснованно определять расчет и распределение сотрудников безопасности в местах массового пребывания людей, а также принимать решение о месте направления группы перехвата и ее составе.

Матрица (2.58) задает ориентированный граф переходов (вероятностный граф маршрутов). В качестве весов ребер рассматриваются значения вероятности (p_{ij}) того, что нарушитель пришел в конечную вершину (j) из начальной (i) (рисунок 2.8).

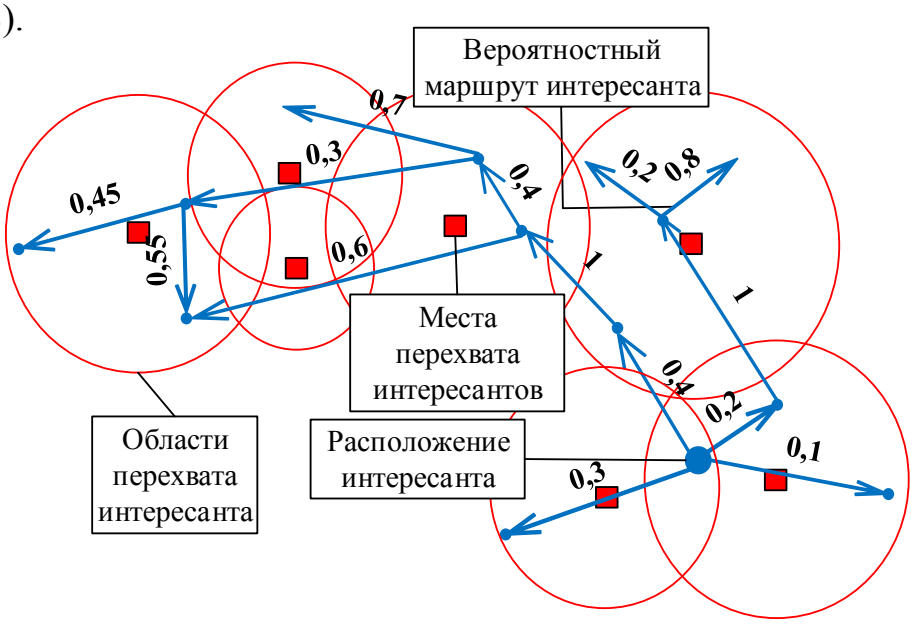


Рисунок 2.8. Вероятностный граф маршрутов нарушителей и зоны размещения сотрудников службы безопасности

Кроме того можно доказать, что при обнаружении интересанта в поле видимости камеры k_0 распределение КОМЦ в момент времени n определяется строкой с номером k_0 матрицы переходных вероятностей в n-ой степени:

$$\vec{p}_{k_0 n} := (P\{\xi_n = 1 \mid \xi_0 = k_0\} \dots P\{\xi_n = m \mid \xi_0 = k_0\}) =$$

$$= \left(p^{(n)}{}_{k_0 1}, \dots, p^{(n)}{}_{k_0 m}\right) = \begin{pmatrix} p^{(n)}{}_{11} & \cdots & p^{(n)}{}_{1m} \\ \vdots & \ddots & \vdots \\ p^{(n)}{}_{m1} & \cdots & p^{(n)}{}_{mm} \end{pmatrix}_{\overrightarrow{k_0}} = \quad (2.98)$$

$$= \{\text{уравнение Колмогорова — Чепмена}\} = \Pi^{n}_{\overrightarrow{k_0}}$$

Таким образом, на основе данного подхода, орган управления обладает информацией о распределении вероятностей местонахождения интересанта в бедующие моменты времени. На основе данного распределения орган управления может выбирать, куда и в каком составе направлять группы перехвата.

Таким образом, выражение (2.92) демонстрирует то, как реакция оператора ИАС, расположение и количество камер в сети видеоконтроля, объем хранилища, количество распознаваемых интересантов влияют на эффективность функционирования ИАС. Более того, данное выражение является вероятностным критерием эффективности ИАС. Оно позволяет при известных математических ожиданиях и дисперсий соответствующих временных интервалах выбрать такие значения описанных параметров, при которых ИАС будет эффективно функционировать. Кроме того, на основе оценки (2.97) могут быть разработаны организационно-технические требования к нормативным значениям времени перехвата и нейтрализации интересанта, что улучшит эффективность защиты объекта.

После того как интересанты обнаружены может возникать задача управления задержанием. Выражение (2.98) определяет распределение вероятностей местоположения интересантов в бедующие моменты времени, что позволяет обоснованно определять количество и распределение сотрудников безопасности в местах массового пребывания людей, а также принимать решение о местах направления группы перехвата и ее составе.

Общая структурная схема модели управления безопасностью представлена на рисунке 2.9. В данной схеме используется разработанная система поддержки управления на базе идентификации по изображению.

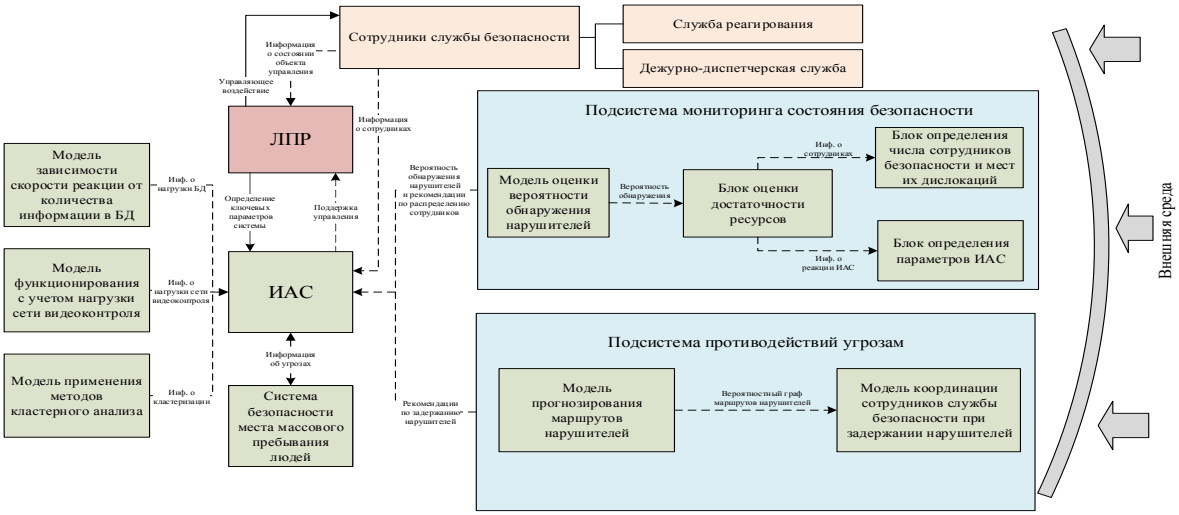


Рисунок 2.9 – Схема модели управления безопасностью людей в местах их массового пребывания

2.6 Вывод по второй главе

В данной части диссертационного исследования синтезированы методы теории управления, теории графов, теории распознавания образов, теории случайных процессов с целью разработки многопараметрической модели информационно-аналитической поддержки управления безопасностью мест массового пребывания людей, оборудованных средствами идентификации по изображению.

Разработана система информационно-аналитической поддержки управления безопасностью при обнаружении и противодействии дестабилизирующим проявлениям интересантов. Кроме того, исследовались способы повышения эффективности данной системы. Эффективность может быть повышена за счет распараллеливания вычислений. В работе доказано, что сеть видеоконтроля можно рассматривать как конечную однородную Марковскую цепь. Данное утверждение позволило разбить множество камер в объединение непересекающихся групп, внутри которых информация об интересантах может обрабатываться последовательно, а вне групп – параллельно.

Также с использованием данной модели возможно построение вероятностного графа маршрутов интересанта. А именно сеть видеоконтроля можно рассматривать в качестве графа, ребра которого несут определенную

нагрузку. В качестве такой нагрузки рассматривается значение вероятности того, что интересант пришел в конечную вершину из начальной. Что позволяет повысить точность и уменьшить время распознавания интересанта следующим образом: при распознавании интересанта рекомендуется сравнивать лицо с уже идентифицированными лицами в смежных вершинах в порядке уменьшения значения метки ребра.

Далее в работе получено выражение, проясняющее влияние количества информации на эффективность системы поддержки управления. Основной вывод из которой – эффективной может быть та система, в которой не превышен верхний порог числа записей в БД. Для того, чтобы соблюсти это условие, одним из решений может стать использование распределенных хранилищ различного типа с применением кластеризации изображений.

Следовательно, необходимо разделять общий массив информации на части (кластеры), что позволит сократить количество операций по сравнению изображений. Данные кластеры должны составлять такую величину, которая позволит иметь необходимый объем информации для распознавания лиц, но количество кластеров должно позволять проводить распознавание за приемлемое время.

Предложенная система поддержки управления позволяет органу управления получать объективную оценку распределения и поведения интересантов, а также координировать силы и средства охраны при противодействии.

Кроме того, на основе разработанной модели сформирована вероятностная оценка эффективности функционирования системы мониторинга дестабилизации, в которой впервые в совокупности учитываются такие параметры, как:

- скорость реакции персонала на событие деструктивного характера;
- переменная скорость движения нарушителя;
- нагрузка сети видеоконтроля;
- объем хранимой информации в базе данных;
- количество анализируемых нарушителей;
- другие параметры автоматизированной системы идентификации.

На основе данной модели могут быть разработаны организационно-технические требования к нормативным значениям времени перехвата и нейтрализации интересанта, что улучшит эффективность защиты объекта.

ГЛАВА 3. РАЗРАБОТКА АЛГОРИТМА И СИСТЕМЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ПОДДЕРЖКИ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

Во второй части для поддержки управления выполнен анализ безопасности мест массового пребывания людей и функционирования автоматизированных средств дистанционной идентификации по изображению с применением математических методов. Для реализации полученных предложений и выводов в конкретных системах поддержки управления необходима разработка новых алгоритмов.

3.1 Структурная схема

Рассмотрим схему модели управления безопасностью, отличающейся использованием предлагаемой ИАС (рисунок 3.1). Архитектура ИАС построена на основании математических моделей представленных во второй главе. Кроме того предложенная архитектура ИАС не ограничивается функционалом способным осуществлять распознавание лиц. Архитектура ИАС расширена на функционал, обеспечивающий определение эмоционального состояния, степени опасности поведения, уровня психологической напряженности и других психофизиологических показателях интересанта. Реализация этого дополнительного функционала представляется возможным в рамках дальнейших научно-исследовательских работ.

ИАС построена на распределенной сетевой архитектуре, состоящий из центральных и локальных систем.

Локальная система включает:

- видеокамеры;
- модуль детектирования, который обеспечивает автоматическое обнаружение изображений лиц в видеопотоке от источника видеосигнала;
- ядро идентификации, которое применяется для сравнения изображение лица интересанта с хранимой информацией о личностях;

- блок кластеризации, который используется для кластеризации хранимой информации и определения центров кластеров;
- локальный сервер с оперативной памятью (далее – ЛОП), который используется для хранения центров кластеров;
- локальную базу данных, которая применяется для долговременного хранения информации об интересантах;
- сенсоры, которые регистрируют психофизиологические показатели;
- аналитический модуль, который используется для отслеживания траектории передвижения, выявления аномального поведения, определения эмоционального состояния и уровня психологической напряжённости;
- сервер запросов, который служит для централизованной обработки аналитических запросов оператора;
- автоматизированные рабочие места операторов, которые обеспечивают доступ к функциям системы по мониторингу событий, настройке параметров локальной системы и вводу информации в БД.

Центральная система включает:

- ядро идентификации, которое применяется для сравнения изображение лиц интересанта, поступающих из локальных систем, с хранимой информацией о личностях;
- блок кластеризации, который используется для кластеризации хранимой информации и определения центров кластеров;
- центральный сервер с оперативной памятью (далее – ЦОП), который используется для хранения центров кластеров;
- центральная база данных, которая применяется для долговременного хранения информации об интересантах;
- сервер запросов, который служит для централизованной обработки аналитических запросов оператора;

- автоматизированные рабочие места операторов, которые обеспечивают доступ к функциям системы по мониторингу событий, настройке параметров центральной системы и вводу информации в БД.

Далее опишем принцип функционирования ИАС: при обнаружении интересанта в режиме «реального времени» осуществляется распознание на основе уникальности биометрии лица, отслеживается и анализируется траектория его перемещения, определяется эмоциональное состояние и уровень психологической напряжённости.

Остановимся более подробно на распознавании интересанта. После обнаружения изображения лица в видеопотоке от источника видеосигнала, оно соотносится с изображениями лиц в хранилище. В результате в БД формируются кластеры, в которых содержатся только похожие изображения. В идеале для скоростного распознавания необходимо, чтобы один кластер соответствовал одному человеку. При этом в каждом кластере необходимо вычислить набор наиболее типичных и качественных изображений лиц (средние значения на кластер).

Таким образом, для поиска интересанта по фотографии с использованием ИАС (или её составной части) достаточно изображение лица сравнить с ограниченным набором изображений (наиболее точно представляющим личность в данном кластере), а не со всеми изображениями в БД.

Для хранения данных в такой системе необходимо использовать новый принцип хранения и обработки. Рассмотрим контролируемый объект, например, аэропорт. С модулей детектирования поступает поток видеоданных, который обрабатывается локальным сервером идентификации, по следующему новому алгоритму хранения и распознавания, который схематично представлен на рисунке 3.2:

Пусть *n* - номер изображения с лицом

1) (n = 1). На вход ядру идентификации подается первое изображение. Для изображения строится математический шаблон лица. Информация

сохраняется в локальном сервере с оперативной памятью (ЛОП). Таким образом, в ЛОП содержится один кластер с центром в единственном изображении лица;

2) (n = 2). На вход ядру идентификации подается второе изображение. Для изображения вычисляются математический шаблон. Шаблон сравниваются с центром единственного кластера:

a. если изображения достаточно похожи, то есть проверяются, соответствуют ли они одной личности, то кластер расширяется полученным изображением. Выбирается центр кластера, который сохраняется в ЛОП, другой представитель кластера сохраняется в ЛБД;

b. если изображения различаются (уровень доверия ниже заданного порога), то есть изображения соответствуют разным личностям, то образуется новый кластер с центром в новом изображении.

3) ($n = m$). Пусть уже есть k кластеров. На вход ядру идентификации подается m-тое изображение. Оно проверяется на схожесть с центрами k кластеров идентифицированных лиц. Причем сравнение осуществляется с уже идентифицированными лицами в смежных вершинах в порядке уменьшения значения метки ребра вероятностного графа маршрутов. Построение вероятностного графа маршрутов описано ранее в параграфе 2.2. В результате:

a. если изображения лица относится к какому-то кластеру, то оно расширяет данный кластер. В кластере выбирается новый центр, т.е. изображение лица, наиболее точно представляющее личность, и оно сохраняется в ЛОП, другие изображения сохраняются в ЛБД;

b. если уровень доверия с каждым из k центров кластеров ниже заданного порога, то считается, что изображение лица соответствует личности, которой нет в ЛБД. Данное изображение образует новый кластер.

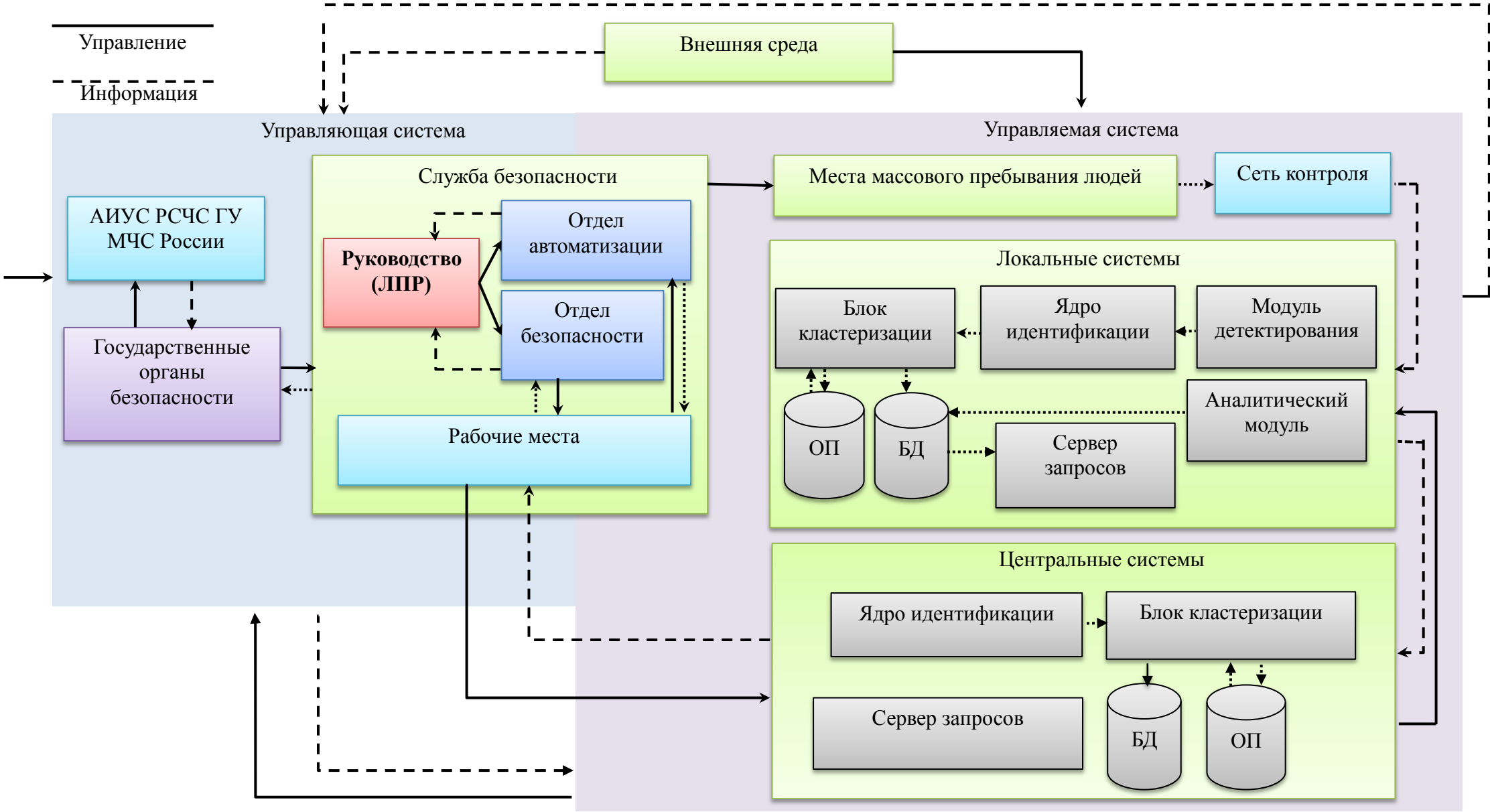


Рисунок 3.1 Схема информационно-аналитической системы поддержки управления

Вход:

- $face_{mi}$ – математический шаблона лица, который был зафиксирован *i*-ой камерой;
- $i \in E_j$, где $E_j = \{i_1 \dots i_g\}$– класс камер полученный в результате применения КОМЦ;
- $face^{ri} \in FC_i$– центр *r*-го кластера, а $FC_i = \{ face^{r1i} \dots face^{rti} \}$– множество центров кластеров, элементы которых зафиксированы на *i*-ой камере.

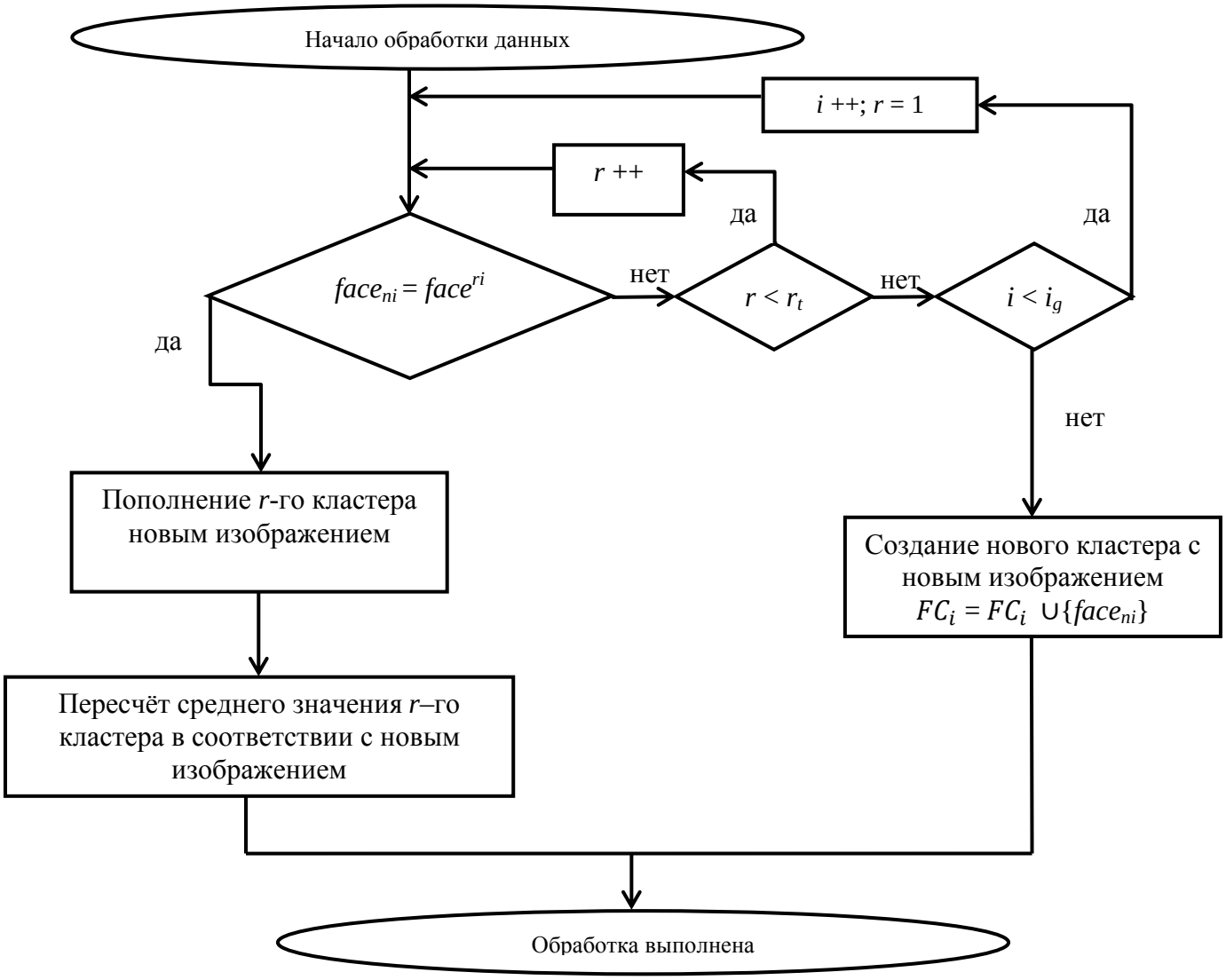


Рисунок. 3.2 Алгоритм хранения и обработки данных ИАС

В ЦБД хранится информация о центрах кластеров из всех ЛБД.

При этом если личность попала в поле видимости камер нескольких контролируемых объектов, например аэропорта, вокзала, станции метро, и образовала кластеры в разных ЛБД, то в ЦБД должен быть образован кластер, состоящий из центров этих кластеров ЛБД.

Для принятия решения о том, какому кластеру принадлежит изображение можно воспользоваться байесовским классификатором [103]. Представим изображения лиц в качестве многомерных случайных величин x_1 и x_2 с нормальным распределением. Рассмотрим две гипотезы:

H_1 = {центр кластера (x_1) и входное изображение (x_2) соответствуют одному человеку};

H_2 = {центр кластера (x_1) и входное изображение (x_2) соответствуют разным людям}. Тогда воспользовавшись оценкой апостериорного максимума, можно рассматривать логарифм отношения функций правдоподобия как меру сходства двух изображений:

$$r(x_1,x_2) = \log(P(x_1 - x_2/ H_1)/ P(x_1 - x_2/ H_2)). \quad (3.1)$$

Синхронизацию данных в центральных и локальных системах предлагается осуществлять следующим образом. В заданные промежутки времени необходимо синхронизировать:

– информацию о фактах регистрации физических лиц, в частности центр кластера из ЛБД, который лучшим образом отображает лицо человека;

– общий каталог, т.е. общий вектор пребываний.

В ЛБД содержится информация о распознавании лиц и значения случайных величин пребываний. Информация о распознавании сгруппирована в кластеры (один человек – один кластер). Таким образом, синхронизация будет выглядеть следующим образом:

1. ЦБД не заполнена. Тогда из любой ЛБД:

a. копируются информация об идентификационных документах и центров кластеров. Таким образом, будет скопирована информация которая лучшим образом отображает лицо человека;

b. для каждого кластера из ЛБД копируются значения общего вектора пребывания в ЦБД.

2. ЦБД заполнена. Тогда для ЛБД, которые не синхронизированы на вход ядру идентификации ЦБД подаются центры кластеров из ЛОП. Центры кластеров из ЛОП сравниваются с центрами кластеров из ЦОП:

a. если уровень доверия выше заданного порога, то считается, что два кластера представляют одно физическое лицо. Согласно идентификатору этого физического лица, сохраняются значения общего вектора пребывания;

b. если уровень доверия ниже заданного порога, то считается, что физическое лицо, которое характеризует кластер из ЛБД, не представлен в ЦБД. Тогда копируется среднее значение кластера и значение общего вектора пребываний в ЦОП и ЦБД соответственно.

Приводимые архитектура ИАС и алгоритм хранения информации соответствует выводам второй главы. Число записей на обработку будет сокращено в десятки раз, следовательно, время обработки изображения сократится.

Одним из перспективных направлений является проведение расчётов по поиску средних значений для каждого из кластеров не в момент поступления нового изображения, а в тот момент, когда ИАС не «занята». Такой момент может наступить во время визуальной обработки данных оператором, либо по окончании выдачи данных из ЦБД в локальные БД.

3.2 Структура и организация хранилища системы поддержки управления

Далее представлена модель хранения информации в базах данных ИАС. Хранилище ИАС построено на распределенной сетевой архитектуре, состоящей из центральных БД (ЦБД) и локальных БД (ЛБД). Хранилище ИАС позволяет своевременно оповещать оператора о личности человека на объекте и его степени опасности.

Предметной областью является объект с достаточно высокой плотностью человеческого потока.

Сохраняемая информация об интересантах включает в себя следующие категории самостоятельных материалов:

1) запись с видеокамер;
2) изображение и математический шаблон лица;

3) информация об эмоциональном состоянии, поведении, уровне психологической напряженности и других психофизиологических показателях интересанта;

4) данные о дате и времени регистрации интересанта;

5) информация об адресе и месте установки видеокамер;

6) идентификационная информация об интересанте;

7) информация о запрашиваемых оператором данных об интересанте.

Приведенные категории информации составляют основу информационной единицы хранения (далее - ИЕХ).

ИЕХ используют в практике построения БД в случаях, когда необходимо установить соответствие с объектами хранения, имеющими сложную структуру. База данных должна быть ориентирована на высокую скорость записи значительного количества информации. Поэтому к ней необходимо предъявлять следующие требования:

1) ориентированность на высокую скорость записи в БД;

2) высокая скорость решения аналитических задач;

3) масштабируемость;

4) запрет изменения данных после обработки и сохранения.

Рассмотрим подходы к построению архитектуры хранилища:

1) централизованное хранение всех данных. Единственное общее хранилище данных о людях, их местах пребывания и метаданных, используемых при распознавании;

2) распределенное хранение данных. Данные о людях, их местах пребывания и служебная информация хранятся в наборе ЛБД.

Каждый подход имеет определённые преимущества и недостатки, рассмотрим их.

Централизованное хранение предусматривает, что данные хранятся на одном узле. Главное преимущество заключается в простоте архитектуры. Пользователю комплекса для получения информации о физическом лице достаточно инициировать запрос в одну БД.

Преимущества данного метода:

1) минимизировано использование сетей при запросах оператора комплекса. Благодаря такой архитектуре, время пересылки информации о видеофиксации физических лиц минимизировано;

2) простота запросов на предоставление информации о видеофиксации физических лиц. Запросы упрощаются за счёт того, что нет необходимости запрашивать информацию из различных источников;

3) отсутствует необходимость хранения информации о ЛБД, в которой содержится информация о месте видеофиксации физического лица. При запросе информации о местах видеофиксации по фотографии отсутствует необходимость обращения в различные ЛБД, например, аэропорта или вокзала.

Недостатки:

1) высокое использование сетей при запросах ЯИ различных мест массового скопления людей;

2) большая нагрузка на одну БД. В результате ЯИ различных мест массового скопления людей будет сохранять информацию в одной БД. Безусловно, с большим количеством мест массового скопления это приведет к превышению верхнего порога числа записей;

3) критическая зависимость от одной БД. Комплекс полностью зависим от одной БД. В случае сбоя ее функционирования, комплекс становится полностью неработоспособен.

Распределенное хранение данных предусматривает, что данные хранятся в базах данных разных узлов. Очевидным недостатком такого подхода является сложность построения и реализации.

Преимущества:

1) независимость работоспособности ЛБД одного узла от работоспособности ЛБД другого узла;

2) минимизировано использование сетей при запросах ЯИ. ЯИ будет обращаться и сохранять информацию в своей собственной БД. Эта БД может находиться на том же сервере, что и ЯИ.

Кроме хранения метаданных, используемых при распознавании, возникает задача хранения значений случайной величины пребываний ξ в адресном пространстве, то есть информации о времени и месте видеофиксации, а также централизованного доступа к этой информации с целью эффективного решения аналитических задач. Для хранения значений случайной величины, необходимо сохранять следующую информацию:

- идентификатор физического лица;
- адрес видеофиксации физического лица;
- время видеофиксации.

Значения случайных величин будут храниться в каталоге (далее − каталог). Рассмотрим полный каталог. В данном каталоге будут храниться значения всех случайных величин со всех узлов (далее − полный каталог).

Рассмотрим возможные варианты хранения каталога:

1) центральное хранение. Единственный полный каталог хранится на отдельном центральном узле. Данный метод хранения данных упрощает запросы оператора комплекса к БД. Для запроса информации о местах видеофиксации пользователю достаточно создать запрос на обращение к каталогу в некой ЦБД. Однако появляется зависимость от центрального узла;

2) полная репликация. Полный каталог хранится на каждом узле. Для запроса информации о местах видеофиксации пользователь комплекса может обратиться к любому узлу с ЛБД. Однако будут использоваться дополнительные ресурсы сети и сервера на синхронизацию данных во всех узлах;

3) частичное секционирование. Каждый узел поддерживает собственный каталог. Полный каталог представляет собой объединение всех этих непересекающихся локальных каталогов. Такая структура неэффективная с точки зрения того, что оператору комплекса при запросе мест видеофиксаций необходимо будет производить опрос ЛБД всех мест массового скопления людей. В случае большого количества ЛБД, этот запрос будет выполняться за достаточно большой промежуток времени. Кроме того, запрос будет создавать лишнюю

нагрузку на ЛБД, в которых нет информации, удовлетворяющей критериям запроса;

4) комбинированное хранение. На каждом узле поддерживается свой локальный каталог. Кроме того, отдельный центральный узел хранит каталог подвекторов случайной величины пребываний.

Рассмотрим более подробно комбинированную структуру хранения каталога. В локальных базах данных хранится каталог значений случайных величин пребываний $\xi_j = \xi_j (a, t)$, а именно следующие значения:

– идентификатор физического лица (значение параметра j);

– адрес видеофиксации физического лица в рамках локального места массового скопления людей (значение параметра a);

– время видеофиксации (значение параметра t).

На ЦБД в общем каталоге хранится округленные значения начальных и конечных координат подвектора $\xi_{jk} = ((a_{jk1},t_{jk1}),.. (a_{jkv},t_{jkv}))$ вектора случайной величины пребываний ξ_j, (далее − общий вектор пребываний), а именно:

– идентификатор физического лица (значение параметра j);

– адрес места массового скопления людей (Аэропорт «Домодедово», «Савеловский вокзал»), в котором состоялась видеофиксация физического лица (округленное значение параметра $a_{jk} = (a_{jk1} \approx ... \approx a_{jkv})$);

– время первой видеофиксации (значение параметра t_{jk1});

– время последней видеофиксации (значение параметра t_{jkv}).

На основании вышеизложенного, предлагается распределенная архитектура хранения данных с комбинированной структурой хранения каталога случайной величины пребываний.

Рассмотрим особенности предложенной системы:

1) простота аналитических запросов на предоставление информации о видеофиксации физических лиц. Запросы упрощаются за счёт того, что нет необходимости запрашивать информацию из различных источников;

2) аналитические запросы пользователей комплекса не создают нагрузку на ЛБД;

3) минимизировано использование сетей при запросах оператора комплекса. Благодаря такой архитектуре, время пересылки информации о значениях случайной величины присутствия минимизировано;

4) ЯИ не запрашивает информацию из центрального сервера и не использует сеть, как в случае с централизованным хранением всех данных;

5) комплекс устойчив к неработоспособности серверов с общим каталогом, а именно в случае сбоя на центральном сервере с общим каталогом, запрос может быть выполнен параллельно на удаленных серверах с локальными каталогами;

6) отсутствует необходимость хранения информации о ЛБД, в которой содержится информация о месте видеофиксации физического лица.

Таким образом, сохраняются все преимущества централизованного хранения данных и нивелируются недостатки.

Далее рассматривается реализация заявленных характеристик хранения информации в виде структур БД. Для этого необходимо задать правила предметной области и сущности ИАС.

Основные правила предметной области:

– одному человеку могут соответствовать несколько изображений;

– одному изображению лица соответствует уникальный математический шаблон;

– одному человеку могут соответствовать несколько идентифицирующих документов;

– одному оператору ИАС может соответствовать несколько запросов;

– одному человеку могут соответствовать несколько запросов в ИАС;

– в один момент времени одному человеку могут соответствовать несколько эмоциональных состояний;

– в один момент времени одному человеку могут соответствовать несколько видов поведения;

– одному уровню напряженности могут соответствовать несколько человек;

– в один момент времени одному человеку соответствуют уникальные показатели датчиков электроэнцефалографии;

– в один момент времени одному человеку соответствуют уникальные показатели пневмографа;

– в один момент времени одному человеку соответствуют уникальная кожно-гальваническая реакция;

– в один момент времени одному человеку соответствуют уникальные показатели сердечно-сосудистой системы и т.д.

Данные правила вводят определенные ограничения на процессы, происходящие в базе данных. В таблице 3.1 определены сущности АС.

Структура ЦБД и ЛБД приведена на рисунках 3.3 и 3.4 соответственно. Описание таблиц и полей ЦБД и ЛБД представлено в Приложении 1. Представленные структура и перечень полей БД раскрывают принцип организации и расположение материалов.

Таблица 3.1 – Сущности ИАС

Сущность	**Сохраняемые параметры**
интересант, попавший в поле деятельности АС	фамилия
	имя
	отчество
	дата рождения
документ, удостоверяющий личность	название
	номер
	фамилия
	имя
	отчество
	пол
	путь в файловой системе к расположению фотопортрета
	другие параметры
история запросов оператора	сведения об операторе
	сведения об интересанте
	дата и время запроса
	параметры запроса
оператор АС	фамилия
	имя
	отчество
	пол
	дата рождения
	номер документа, удостоверяющий личность

математический шаблон изображения лица	матрица математического шаблона
	метод построения шаблона
	изображение
история местоположений интересанта	идентифицирующие сведения об интересанте
	дата и время
	адрес местоположение
ЛБД	IP-адрес
	географический адрес
	параметры
психофизиологическое состояние интересанта	поведение
	эмоциональное состояние
	степень солевых выделений
	напряженность
	уровень тремора
	величина зрачков
	температура
	удельная плотность
	другие параметры
показатели полиграфа	вопрос
	ответ
	степень солевых выделений
	величина зрачков
	уровень тремора
	напряженность
	кожно-гальванический рефлекс
	показатель электроэнцелографии
	состояние сердечно-сосудистой системы
	температурные характеристики
	показатели пневмографа

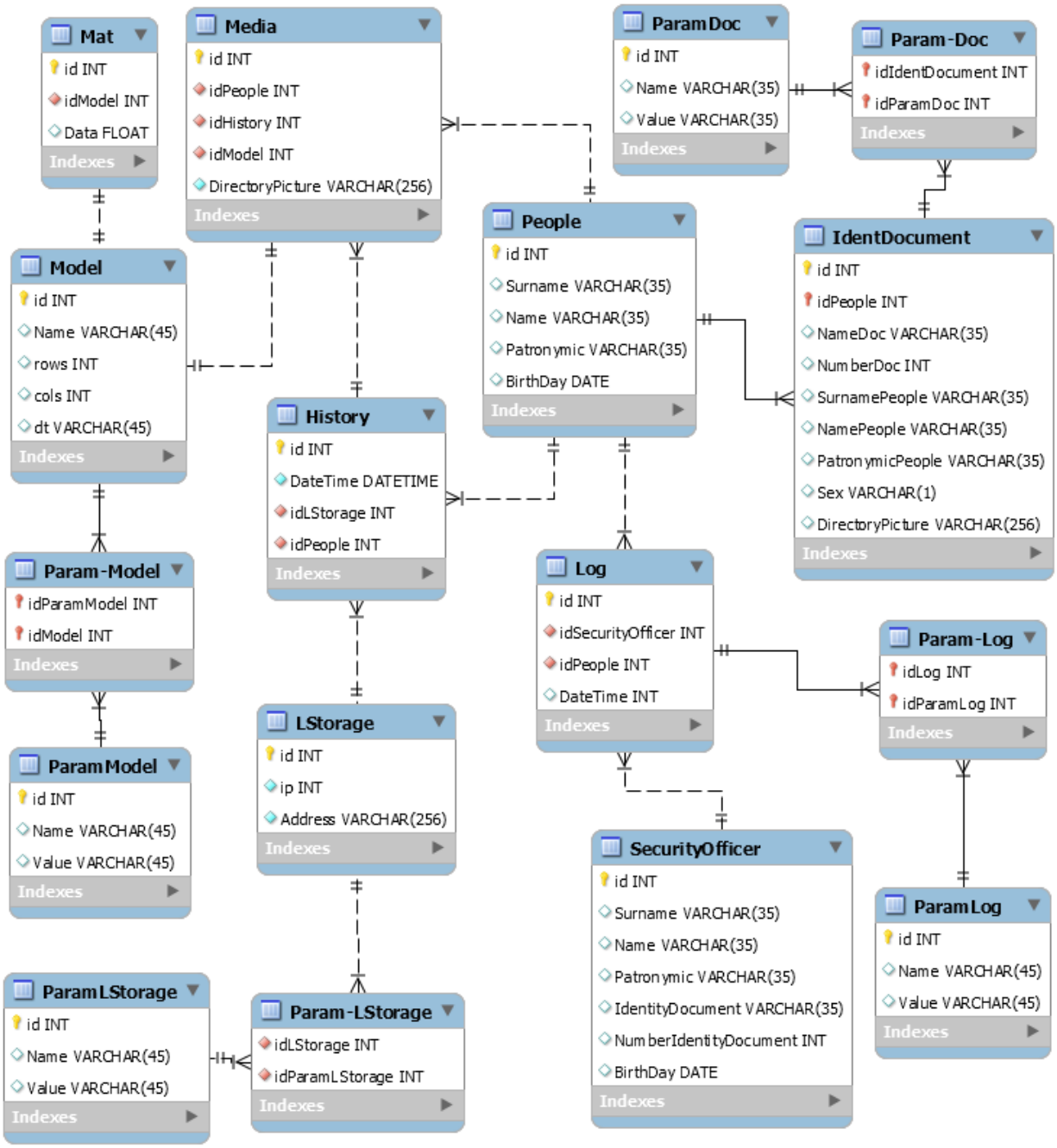


Рисунок 3.3 Структурная схема ЦБД

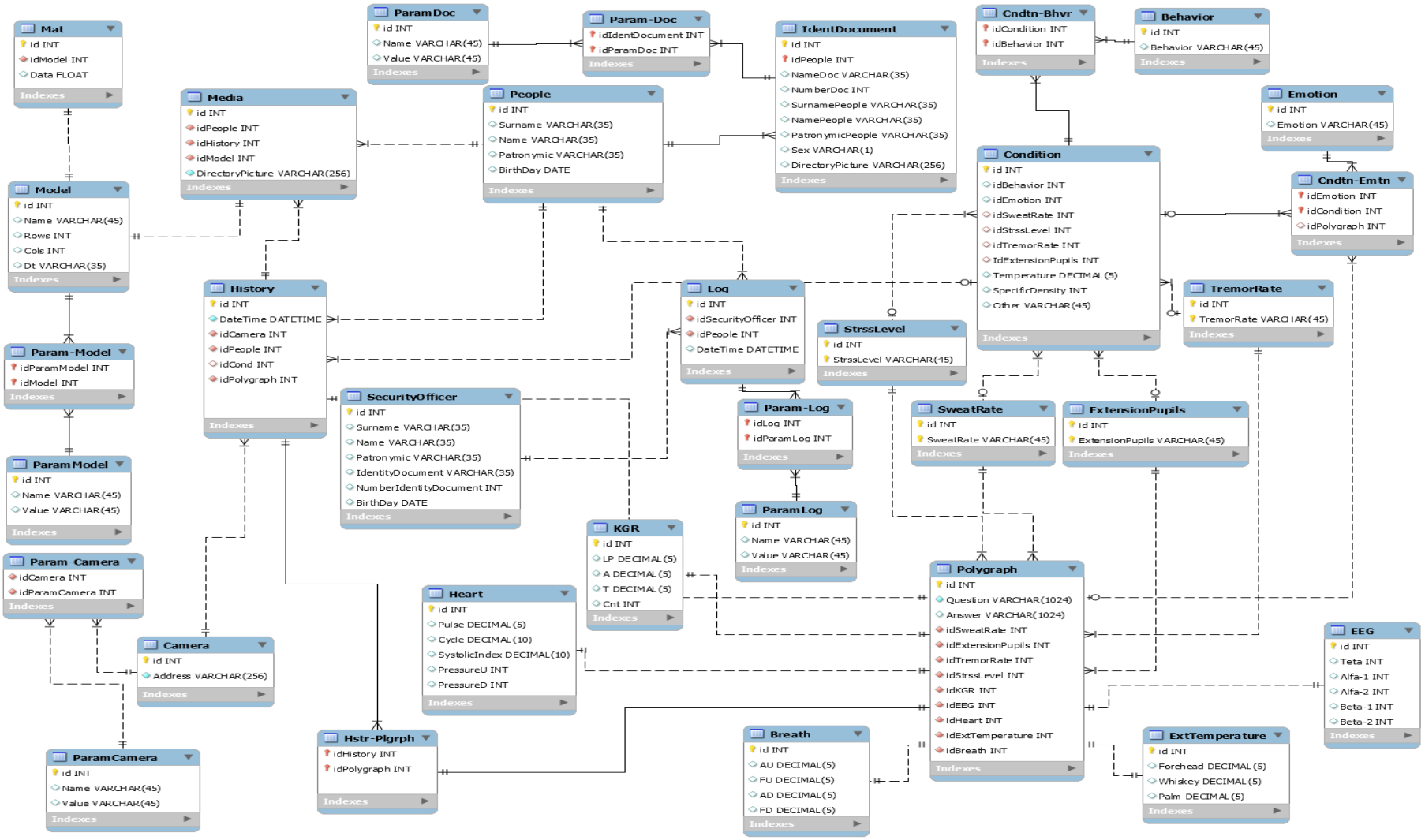


Рисунок 3.4 Структурная схема ЛБД

3.3 Двухуровневый гибридный алгоритм распознавания лиц в системе поддержки управления

Стремительное развитие компьютерных технологий и появление все новых возможностей использования вычислительных устройств позволили в значительной степени усовершенствовать методы распознавания лиц на основе компьютерного зрения. Тем не менее, нельзя с полной уверенностью говорить, что компьютер способен полностью заменить человека при решении сложных задач распознавания.

В данной работе предлагается двухуровневый гибридный метод распознавания лиц (ДГМ), основанный на построенной модели нагрузки сети видеоконтроля (см. п.2.2) и когнитивных механизмов человеческого зрения.

Сеть видеоконтроля представляется конечной однородной Марковской цепью, в которой элементами фазового пространства являются идентификаторы камер. Тогда множество идентификаторов камер распадается на не пересекающиеся классы. Таким образом, сеть видеоконтроля можно рассматривать в виде ориентированного графа возможных маршрутов передвижения интересанта. Вершинами графа являются места видеофиксации (вход, касса и прочее). Каждое ребро графа помечено меткой, значение которой является вероятностью того, что интересант в предыдущий момент времени находился в начальной вершине, при условии, что сейчас он находится в конечной вершине. Также было доказано, что если при распознавании интересанта сравнивать лицо с уже идентифицированными лицами в смежных вершинах в порядке уменьшения значения метки ребра, то точность и скорость распознавания повышается.

Однако при такой процедуре наиболее критично точное распознавание интересанта в начальной вершине графа, так как некорректное распознавание в данной вершине приведет к ошибкам во всех остальных вершинах.

Во всех вершинах графа, за исключением начальных, предлагается использовать МГК. В сочетании с вероятностным графом маршрутов МГК продемонстрировал достаточно хорошую точность и скорость распознавания.

Для повышения точности распознавания в начальной вершине вероятностного графа маршрутов предлагается использовать двухуровневый метод (ДМ). В ДМ используются холистический и локальный методы распознавания.

В соответствии с психологическими исследованиями Олива и Торалба [123] механизмов, лежащих в основе человеческого зрения, локальные и холистические признаки используются в человеческом восприятии, но играют разные роли. В гипотезах [122] предполагается, что человеческое восприятие обрабатывают холистические признаки раньше, чем локальные. В холистических признаках содержится статистическая сводка о пространственных свойствах лица, описывающая его общие контуры и текстуру. С другой стороны, известно, что в локальных признаках содержится подробное описание отдельных черт лица.

Алгоритм ДМ [109] подразумевает два последовательных этапа. На первом этапе выполняется поверхностное распознавание, основанное на МГК, при этом расстояние между эталонным изображением и проверяемыми изображениями используется для измерения точности распознавания. В случае если расстояние между проверяемым изображением и центрами кластеров приблизительно одинаково, то используется МГЛБШГ. При использовании МГЛБШГ уменьшается число проверяемых изображений посредством выбора первых n изображений, после сортировки их в порядке возрастания степени сходства с эталонным изображением. При увеличении количества проверяемых изображений ожидается уменьшение вероятности ошибки, но неизбежно увеличение вычислительной нагрузки.

Преимущество данной стратегии «от поверхностного до детального распознавания» является уменьшение вычислительной нагрузки; после первого этапа сохраняется только небольшое количество проверяемых изображений. Эта

стратегия наиболее эффективна, когда на последнем этапе используются сложные вычислительные методы, наподобие фильтрации Габора.

Предложенный подход к распознаванию в начальной вершине имеет гибкую конструкцию, что позволяет закончить процедуру распознавания на первом этапе с использованием МГК. В экспериментах предложенный метод показал свою большую эффективность с точки зрения не только скорости вычислений, но и точности распознавания лиц в условиях изменения освещенности по сравнению с алгоритмами распознавания, основанными на МГК и вейвлетах Габора.

Для функционирования системы распознавания необходимо хранить в БД изображение лица и представление в виде главных компонент, а для центров кластеров еще и представление в виде гистограмм локальных бинарных шаблонов Габора.

Алгоритм функционирования системы распознавания представлен блок-схемой на рисунке 3.5. Он отличается от обобщенного алгоритма работы системы распознавания лиц и более полно отражает наличие необходимости строить меньшие по размеру БД и применять меньшую частоту сравнений с эталоном.

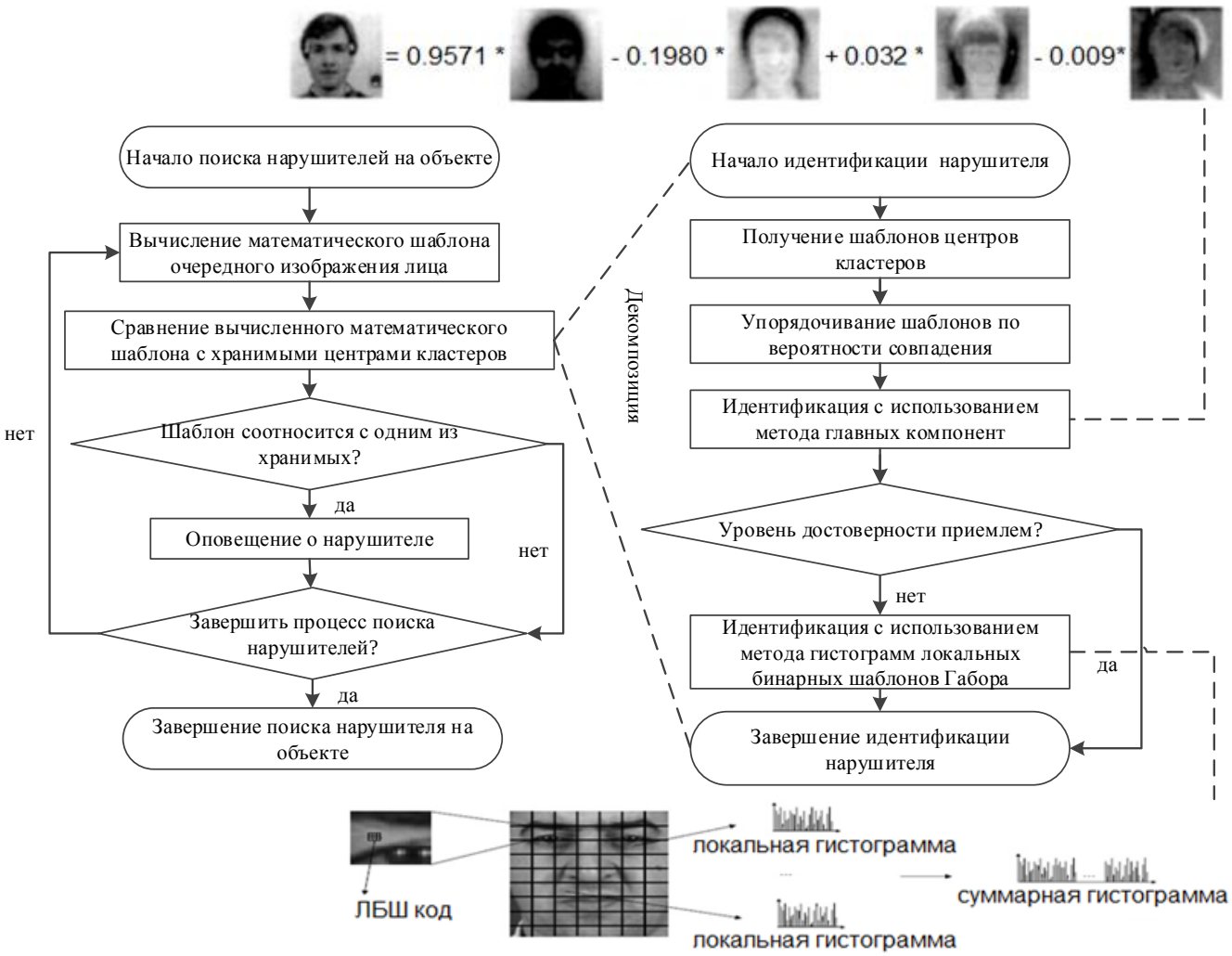


Рисунок 3.5.– Блок-схема усовершенствованного алгоритма идентификации на основе уникальности биометрии лица

3.4 Подход к поиску в хранилище системы поддержки управления

Для улучшения характеристик системы можно использовать алгоритм поиска изображений лиц в БД, так как при необходимости осуществить поиск лица по входной фотографии, в представленной ИАС достаточно сравнить фотографию только с достаточно небольшим набором изображений (центрами) каждого кластера.

Алгоритм поиска изображений лиц в БД:

1) Вычислить математический шаблон изображения лица.

2) Произвести сравнение математического шаблона изображения лица с шаблонами центров кластеров в ЦОП.

3) Если уровень доверия выше заданного порога, предоставить оператору комплекса изображения личности и информацию об идентификационных документов. Данная информация будет получена как из ЦБД, так и из ЛБД.

Замечу, что кластер в БД соответствует одной человеческой личности, а элементы кластера соответствуют фотографиям этой личности. И что для центра кластера уже вычислены математические шаблоны.

В рамках предлагаемой архитектуры поиск изображений лиц по фотографии будет обладать низкой вычислительной сложностью, а именно O(n), где n – это количество кластеров в ЦБД, то есть количество физических лиц попавших в поле видимости видеокамер. При этом O(1) – потребность в вычислительных ресурсах, определяемая для расчёта функции подобия для одного кластера. Соответственно, O(n) – та же потребность для n кластеров.

3.5 Алгоритмы решения задач управления безопасностью

Для ответа на современные вызовы, стоящие перед сотрудниками службы безопасности, уже недостаточно просто организовать систему видеонаблюдения. Эффективное обеспечения безопасности требует автоматизации задач, стоящих ежедневно перед сотрудником службы безопасности. Это сократит время реагирования на изменение оперативной обстановки и улучшит показатели раскрываемости при задержании лиц, которым правоохранительные органы должны уделить повышенное внимание в «реальном времени».

Существующие системы видеонаблюдения с биометрической идентификацией в сфере безопасности ([125], [105], [132]) не предназначены для анализа статистической информации об интересанте, например, такой, как места пребывания. Фактическое их назначение – оказание помощи сотрудникам подразделений безопасности в наблюдении за текущей обстановкой на объекте и автоматическое выявление интересантов по заданной заранее биометрии лица. В таких системах данные хранятся в виде видеофайлов, а не в структурированном виде. Но объем собранной информации по такому городу, как Москва составляет до 10 экзабайт (2^{60} байт = 2^{20} терабайт) информации в сутки ([25]). Даже для

хранения такого количества информации требуются огромные вычислительные ресурсы, не говоря уже об анализе ее оператором и расчет статистической информации об интересанте. Описанный недостаток может повлечь потерю значимой информации о потенциально опасном лице и снизить уровень безопасности в местах массового пребывания людей.

Далее предлагается аналитическая модель статистических задач, стоящих перед сотрудником службы безопасности. От показателей точности и скорости их решения зависит эффективность обеспечения правопорядка и профилактики правонарушений.

Без потери общности предполагается, что сотруднику службы безопасности известна фотография интересанта, и существует база данных, в которой накапливаются и хранятся значения случайных величин описанных ниже. Структура БД представлена ранее. Рассмотрим подробно статистические задачи и разработанные автором их математические описания и решения. Формализация указанных задач и решений осуществляется впервые.

1. Определение мест пребываний.

Данная задача подразумевает привязку данных интересанта к местам его пребывания и частоте его пребывания в заданных местах в определенные периоды времени.

Рассмотрим случайную величину пребываний j-того интересанта ξ_j по адресному пространству с набором параметров (a,t)

$$\xi_j = (a, t), \tag{3.1}$$

где a – адрес пребывания человека, t – начальное (зарегистрированное оборудованием) время его пребывания по этому адресу. Данная случайная величина характеризует места пребывания человека с учетом времени.

Алгоритм поиска мест видео фиксации человеческой личности по изображению лица можно описать следующим образом (рисунок 3.6):

Вход:

- изображение лица (фотография, фоторобот);
- анализируемый временной промежуток.

Выход: значение случайной величины пребывания в адресном пространстве.

Алгоритм:

1) вычислить математический шаблон изображения лица;
2) произвести сравнение вычисленного математического шаблона с хранимыми центрами кластеров в ЦОП;
3) если уровень доверия выше заданного порога:
    a. в случае если оператору комплекса требуется глобальное представление информации в масштабе мест массовых скоплений людей, то предоставить оператору комплекса список местоположений искомой личности с указанием времени из ЦБД (таблица 3.2);
    b. в случае если оператору комплекса требуется детальное представление информации, то предоставить список местоположений искомой личности с указанием времени из ЛБД с использованием ключей из ЦБД (таблица 3.3).

Таблица 3.2 - Выходные данные при реализации алгоритма поиска мест видеофиксации человеческой личности по изображению при глобальном представлении

ФИО	Адрес	Начальное время	Конечное время
Иванов И.И.	Савеловский вокзал	2015-08-10 14:52	2015-08-10 15:13
Иванов И. И.	Аэропорт Шереметьево	2015-08-10 17:35	2015-08-10 21:34

Таблица 3.3 - Выходные данные при реализации алгоритма поиска мест видеофиксации человеческой личности по изображению при детальном представлении

ФИО	Адрес	Время	Ссылка на изображение
Иванов И.И.	Савеловский вокзал, Касса №1	2015-08-10 14:52	Фото №1
Иванов И. И.	Савеловский вокзал, Турникет	2015-08-10 15:05	Фото №2
Иванов И.И.	Савеловский вокзал, Платформа №1, Путь №3	2015-08-10 15:13	Фото №3

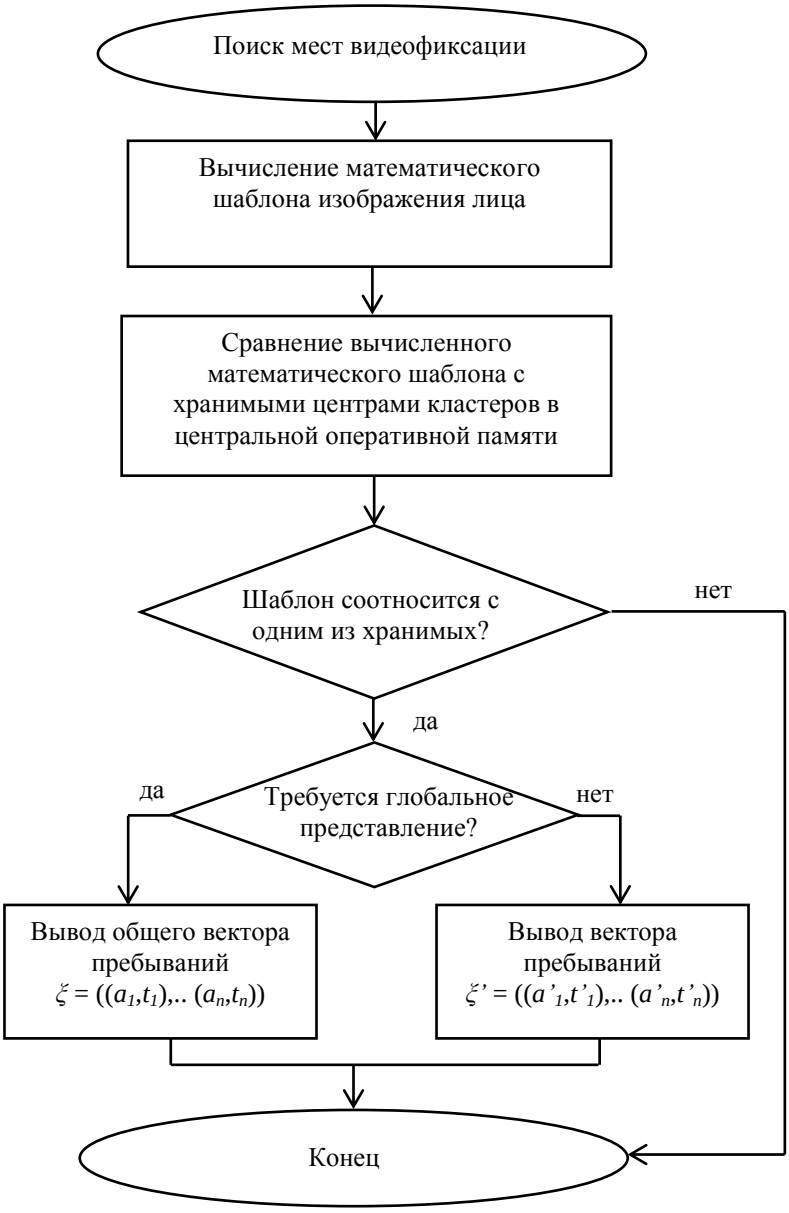


Рисунок 3.6. Блок-схема алгоритма определения мест пребываний.

2. Определение предположительных мест пребывания интересанта.

Рассмотрим случайную величину пребываний интересанта (3.1). Тогда даже если нам известна только часть значений данной случайной величины $\xi_j(a, t)$, применив интерполирование и воспользовавшись алгоритмами построения маршрутов передвижения, можно определить промежуточные значения указанной случайной величины.

3. Выявление связей интересанта (рисунок 3.7).

Как правило, при обнаружении человека, подозреваемого в преступлениях, может возникнуть задача анализа его связей. В контексте существования БД с видеофиксацией людей, поиск связей сводится к поиску попутчиков.

С математической точки зрения возникает задача установки различия между случайными и устойчивыми попутчиками. В контексте исследования можно рассматривать только устойчивых попутчиков. В эту категорию попадают два вида людей:

- люди, с которыми был достаточно продолжительный общий путь;
- люди, с которыми может быть не продолжительный общий путь, но периодический (например, коллеги по работе).

Рассмотрим последовательно решение задачи для обеих категорий граждан. Для тех людей, у которых был достаточно продолжительный общий путь, можно предложить следующую модель решения:

пусть анализируемый человек, для которого мы будем искать попутчиков, имеет случайную величину пребываний в адресном пространстве

$$\xi = ((a_1,t_1),.. (a_n,t_n)), \quad (3.2)$$

где a_i – адрес пребывания человека, t_i – начальное (зарегистрированное оборудованием) время его пребывания по этому адресу, n – количество зарегистрировавших интересанта камер. Будем для краткости называть её адресной характеристикой.

Зададим приемлемое значение, на которое может различаться время видеофиксации Δt. Пусть другой человек, возможно попутчик, попал в зону действия тех же камер. Тогда для него адресная характеристика имеет следующий вид:

$$\zeta = ((a_1',t_1'),.. (a_m',t_m')), \quad (3.3)$$

при этом m – число участвующих в расчёте камер, в поле действия которых попал человек. Значения a_i' и t_i' аналогичны значениям в (3.2).

Для поиска человека с адресной характеристикой (3.2), который будет с высокой долей вероятности попутчиком другого человека с адресной характеристикой (3.3), необходимо найти соответствие их характеристик. С математической точки зрения это означает, что случайная величина пребываний (3.2) имеет подвектор

$$\xi_k = ((a_{k1},t_{k1}),.. (a_{kv},t_{kv})), \quad (3.4)$$

а случайная величина (3.3) подвектор

$$\zeta_p = ((a_{p1}',t_{p1}'),.. (a_{pv}',t_{pv}')), \quad (3.5)$$

где p и k – счётчики камер, а v – их количество, участвующее в расчёте. Для них должна выполняться группа условий $\hat{W}$, о которых известно, что

$$\hat{W} = \begin{cases} a_{ki} = a_{pi}, \forall\, i=1\ldots v \\ \\ t_{ki} - t_{pi} < \Delta t, \forall\, i=1\ldots v \end{cases}. \quad (3.6)$$

Учитывая первое равенство в группе условий $\hat{W}$, можно говорить о разности величин адресных характеристик ξ_k и ζ_p в виде

$$\xi_k - \zeta_p < \Delta t, \quad (3.7)$$

где Δt – допустимая разница во времени между видеофиксацией анализируемых людей.

При этом длину подвекторов ξ_k и ζ_p (значение v), временной промежуток времени (значение $t_{k1} - t_{pv}$), а также значение промежутка времени, за который необходимо установить соответствие адресных характеристик попутчиков, задает оператор комплекса.

Для тех людей, которые могут иметь не продолжительный общий путь, но периодический, можно предложить следующую модель решения:
пусть анализируемый человек имеет случайную величину пребываний

$$\xi = ((a_1,t_1),.. (a_n,t_n)), \quad (3.8)$$

адресная характеристика другого человека

$$\zeta = ((a_1',t_1'),.. (a_m',t_m')), \quad (3.9)$$

тогда необходимо найти у ξ такие подвектора

$$\xi_{k1} = ((a_{k1},t_{k1}),\ldots,(a_{kv},t_{kv}))\ldots \xi_{dr} = ((a_{d1},t_{d1}),.. (a_{dv},t_{dv})), \quad (3.10)$$

а у ζ такие подвектора

$$\zeta_{p1} = ((a_{p1}',t_{p1}'),.. (a_{pv}',t_{pv}')),\ldots,\zeta_{zr} = ((a_{z1}',t_{z1}'),.. (a_{zv}',t_{zv}')), \quad (3.11)$$

что для каждой пары подвекторов из (3.10) и (3.11) должны выполняться условия, о которых известно, что:

$$\xi_{ki} - \zeta_{pi} < \Delta t, \forall\, i=1\ldots r, \quad (3.12)$$

где Δt – допустимая разница во времени между видео фиксацией анализируемых людей, r – количество встреч анализируемых людей. Параметры Δt и r задает оператор комплекса.

Таким образом, накопление и хранение информации о значениях представленных случайных величин в адресном пространстве позволит существенно сократить время решения описанных статистических задач сотрудниками службы безопасности. Создание систем безопасности, в которых возможно максимально автоматизировать задачи сотрудников службы безопасности, в частности поиск и составление списков потенциально опасных посетителей мероприятий, крайне актуально в настоящее время.

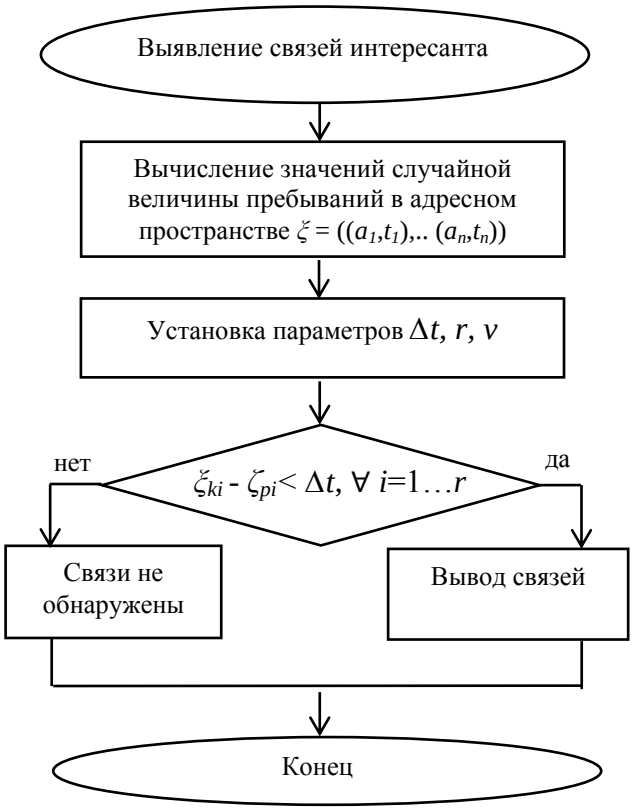


Рисунок 3.7. Блок-схема алгоритма выявления связей интересанта.

Разработанная модель позволит повысить эффективность распознавания лиц, выявления их сообщников, и вследствие этого повысить безопасность в местах массового пребывания людей.

3.6 Алгоритм управления действиями службы безопасности

В качестве возможного примера реализации представленных в исследовании моделей и алгоритмов рассмотрим возможные макеты действий оператора и руководителя группы объектов наблюдения при применении ИАС.

Анализ соответствующих нормативных документов показал, что в целом они направлены на уточнение требований к системам видеонаблюдения и видеоанализа на объектах инфраструктуры мест массового скопления людей ([60], [56]). Однако не существует нормативных документов, регулирующих действия руководителя объекта и оператора системы видеонаблюдения и видеоанализа по выявлению потенциально опасных лиц. Кроме того, опрос руководителей территориальных органов управления МЧС, МВД России и соответствующих подразделений местных органов власти, использующих в своей работе различные системы видеонаблюдения и видеоанализа, продемонстрировал, что реальных алгоритмов действий в этих организациях в настоящий момент нет. Их действия по эксплуатации систем такого вида заключаются в апостериорном анализе произошедших событий, а действия в реальном времени не регламентируются. Поэтому автором разработаны алгоритмы, которые могут быть использованы в качестве основы для создания соответствующих руководящих документов. Представленные макеты действий изначально подразумевают наличие на объекте ИАС, способной в автоматизированном режиме распознавать лица. Однако макеты действий могут быть адаптированы к ситуации с наличием на объекте стандартной системы видеонаблюдения, но при этом эффективность сотрудников службы безопасности, а именно скорость обработки данных, будет более низкой.

Остановимся на разработанных алгоритмах. На рисунке 3.8 представлен блок-схема алгоритма поддержки управления, относящийся к оценке вероятности обнаружения нарушителя службой безопасности.

Рисунок 3.8. Блок-схема оценки оперативности реагирования службы безопасности

Алгоритм управления действиями службы безопасности представлен на рисунке 3.9.

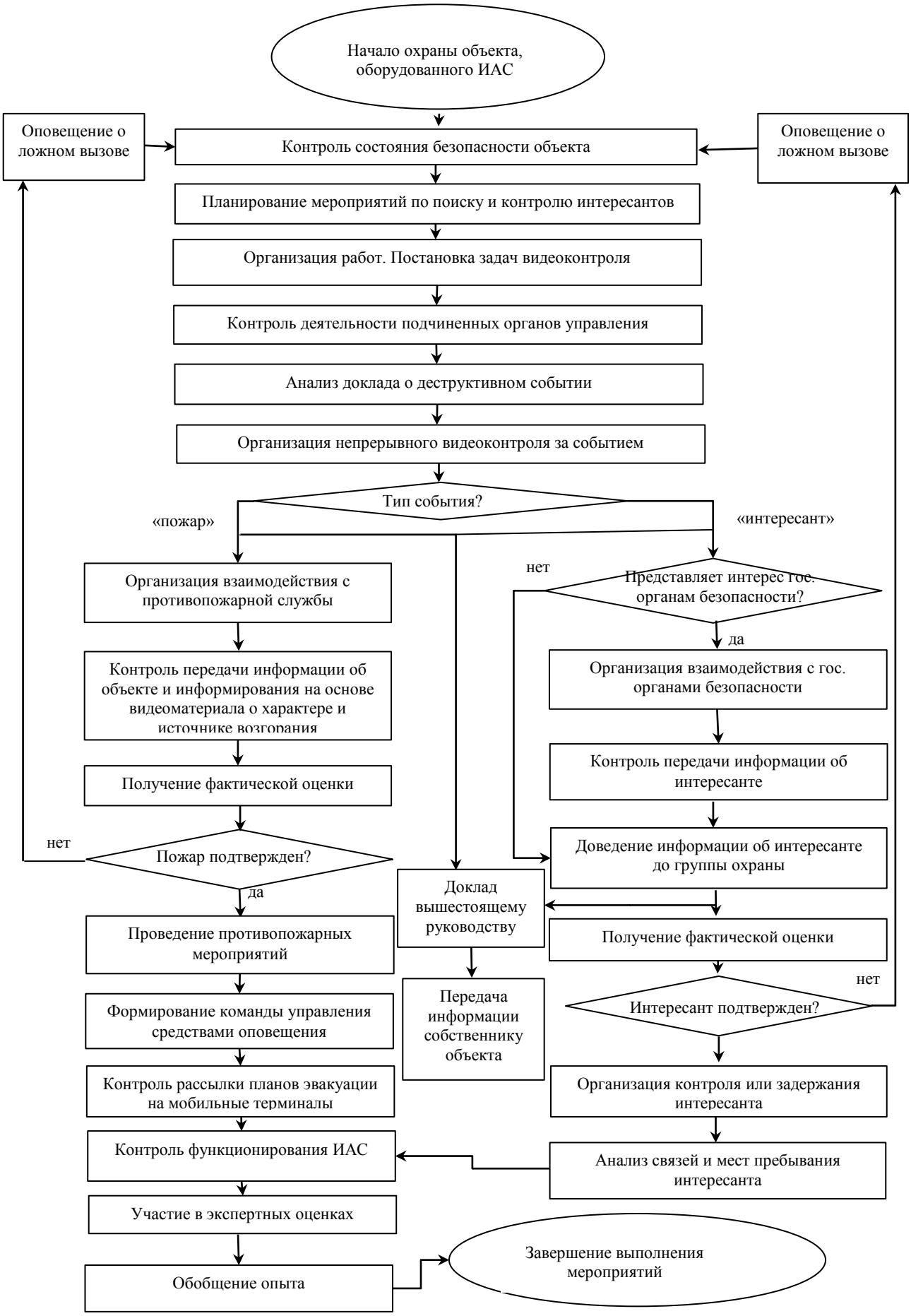


Рисунок 3.9. Алгоритм управления действиями службы безопасности

На рисунке 3.10 представлен блок алгоритма поддержки управления, с использованием которого ЛПР может обоснованно определять число сотрудников безопасности и их распределение, а также принимать решение о составе группы перехвата и месте ее направления.

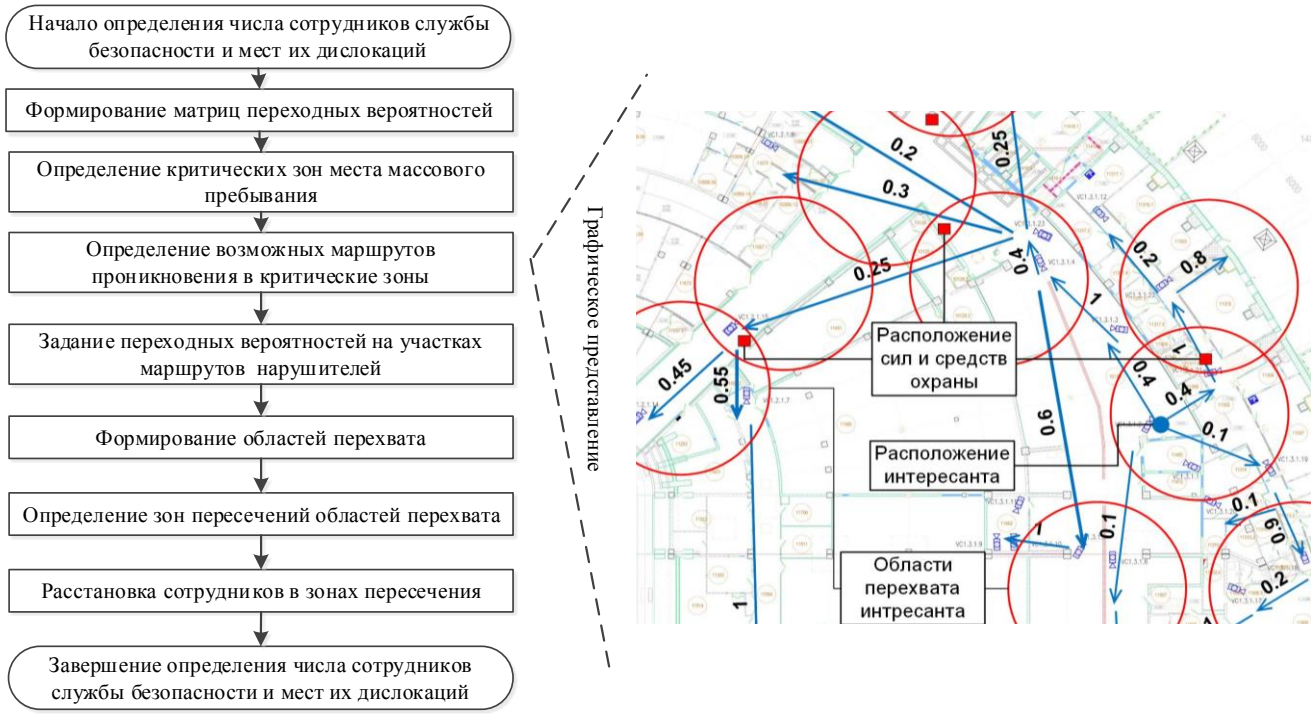


Рисунок 3.10 – Блок-схема и графическое представление распределения сотрудников службы безопасности

Рассмотрим действия руководителя объекта (группы объектов), на котором эксплуатируется ИАС. Предполагается, что при стандартном развитии событий руководитель планово производит оценку обстановки на объекте, что в частности подразумевает сбор информации о выявленных ПОЛ и событиях на объекте, а также о возможных местах появления ПОЛ из различных источников. С учетом полученной информации осуществляется постановка задач операторам по ведению наблюдения на объекте, выявлению ПОЛ и поиску интересантов. Также необходимо осуществлять взаимодействие с другими соответствующими подразделениями по поиску интересантов и выявлению ПОЛ. Важным этапом является получение докладов от подчиненных о ходе выполнения задач и информации от других заинтересованных подразделений. На основе анализа данной информации необходимо принимать дальнейшие решения. Схематично

основные действия руководителя организации представлены на рисунке 3.11 и подробно описан в приложении 2.

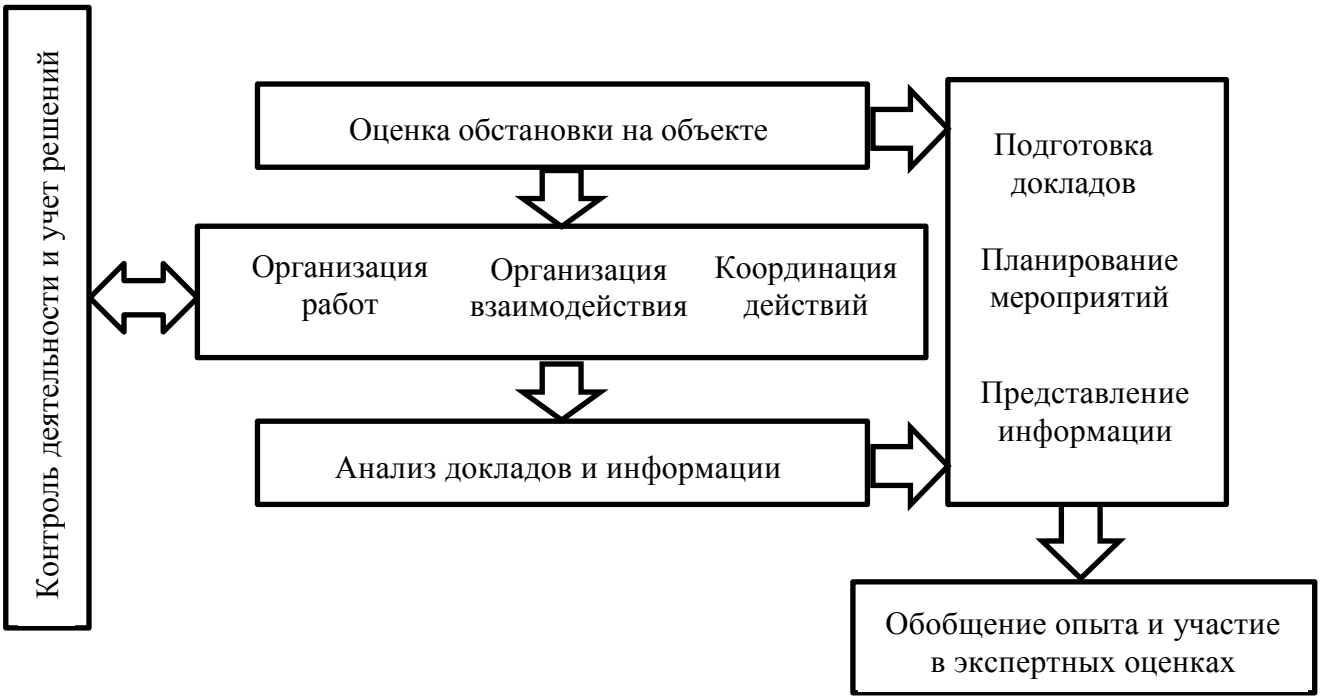


Рисунок 3.11 Алгоритм действий руководителя объекта (группы объектов) при эксплуатации ИАС

Также в приложении 2 представлен перечень предлагаемых действий оператора ИАС. Можно выделить две основных задачи оператора: первая заключается в видеонаблюдении и оценке текущей обстановки на объекте, вторая – в поиске интересантов, поведение которых в настоящий момент не вызывает подозрений, однако стоит задача их обнаружения (например, по причине амнезии интересанта). Кроме того, в обязанности оператора входят традиционные задачи, например, доведение информации до руководства. Схематично основные действия оператора представлены на рисунке 3.12.

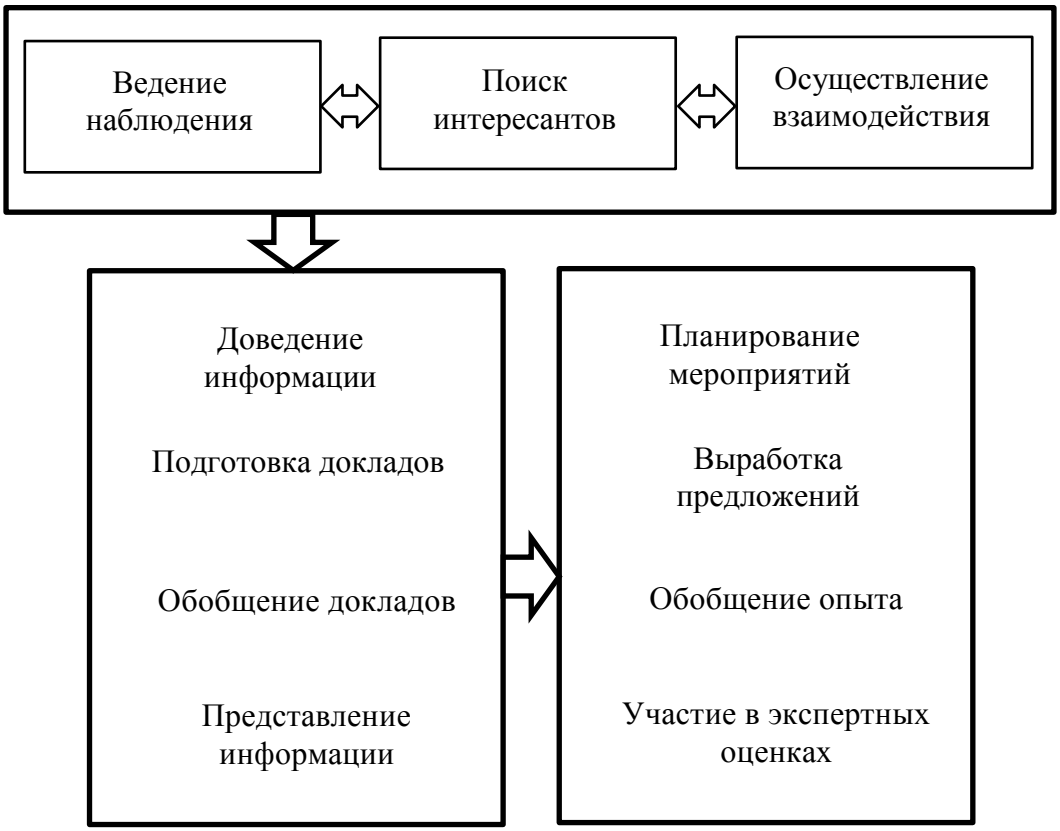


Рисунок 3.12. Алгоритм действий оператора при эксплуатации ИАС

Таким образом, в данной работе впервые приведены разработанные автором алгоритмы действий по обеспечению правопорядка и профилактики правонарушений руководителя объекта (группы объектов) и оператора системы видеонаблюдения и видеоанализа. Данные алгоритмы позволят повысить эффективность выявления ПОЛ в местах массового скопления людей в режиме «реального времени» и могут быть использованы в качестве базовых элементов, создаваемых в будущем соответствующих руководящих документов.

3.7 Вывод по третьей главе

Данная часть содержит практические рекомендации по реализации выводов, полученных в предыдущей части.

С целью повышения эффективности управления предложены: новая структурная схема ИАС, новые структуры распределенных БД, новый двухуровневый гибридный метод распознавания лиц, новые алгоритмы поиска изображений лиц в хранилище, новые алгоритмы поиска, анализа

местоположения и связей интересанта, алгоритмы действий руководителя объекта и оператора при эксплуатации ИАС.

Структурная схема ИАС разработана на основе математических моделей, представленных во второй главе. Данная схема расширена на функционал, обеспечивающий определение эмоционального состояния, степени опасности поведения, уровня психологической напряженности и других психофизиологических показателей интересанта. ИАС построена на распределенной сетевой архитектуре, состоящий из центральных и локальных систем.

Основной принцип функционирования заключается в осуществлении детектирования деструктивного события, идентификации человека на основе уникальности биометрии лица, отслеживании траектории перемещения, определении эмоционального состояния и уровня психологической напряженности в момент обнаружения.

Далее в данной работе предложен двухуровневый гибридный алгоритм распознавания лиц, основанный на построенной модели с учетом нагрузки сети видеоконтроля, модели применения методов кластерного анализа к распознаванию лиц и когнитивных механизмов человеческого зрения. На первом этапе выполняется поверхностное распознавание, основанное на методе главных компонент, если этого не достаточно, то используется алгоритм более детального распознавания – метод гистограмм локальных бинарных шаблонов Габора.

Кроме того, за счет использования кластерного подхода в предложенном методе изображение интересанта сравнивается не со всем массивом изображений, а только с теми, которые наиболее качественно отображают человеческое лицо. Благодаря представлению сети видеоконтроля в виде конечной однородной Марковской цепи, изображения сравниваются в порядке уменьшения вероятности успешного распознавания.

Далее в данной работе предложен новый алгоритм быстрого поиска изображений лиц в хранилище. Благодаря использованию модели применения методов кластерного анализа к распознаванию лиц, для поиска интересанта по

фотографии достаточно изображение лица сравнить с ограниченным набором изображений, а не со всеми изображениями в хранилище.

Для ответа на современные вызовы, стоящие перед сотрудниками службы безопасности, уже недостаточно просто организовать систему видеонаблюдения. Эффективное обеспечение безопасности требует автоматизации задач, стоящих ежедневно перед сотрудником службы безопасности. В данной работе впервые предлагаются алгоритмы решения статистических задач, стоящих перед сотрудником службы безопасности: определение фактических и вероятных мест пребываний, а также выявление вероятных связей интересанта.

Далее в данной работе впервые рассмотрены возможные алгоритмы действий сотрудников и руководителя группы объектов при эксплуатации ИАС. Разработанные алгоритмы могут быть использованы в качестве основы для создания соответствующей законодательной базы.

ГЛАВА 4. РЕАЛИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ПОДДЕРЖКИ

В данной части исследования представлены практические результаты применения разработанных в исследовании модели и алгоритма.

4.1 Экспериментальная проверка системы информационно-аналитической поддержки управления безопасностью

Для экспериментальной проверки предлагаемых результатов разработано ПО, в котором реализованы:

1) новый гибридный метод распознавания лиц;
2) новые структуры хранения информации об интересантах в БД;
3) новые алгоритмы скоростного поиска информации в БД на основе распознавания образов с учетом кластеризации;
4) новые алгоритмы анализа мест пребывания и связей интересанта.

Данное ПО реализовано с использованием СУБД Microsoft SQL Server 2012 и инструментального средства C++ и C# в среде программирования Microsoft Visual Studio 2012. В качестве аппаратной составляющей использовалась ЭВМ с оперативной памятью 16 Гб и процессором Intel Xeon CPU X5650.

Входная информация для проверки полученной зависимости скорости реакции и надежности от объема данных в хранилище взята из БД Color FERET [4]. Данная БД создавалась в экспериментальных целях под контролем Агентства по перспективным оборонным научно-исследовательским разработкам США (DARPA) и Национального института стандартов и технологий США (NIST). В качестве хранилища использовались БД и ОП.

В результате проверки полученной зависимости скорости и надежности реакции от объема данных в хранилище получены следующие зависимости времени распознавания и ОРС от количества изображений лиц в БД и ОП.

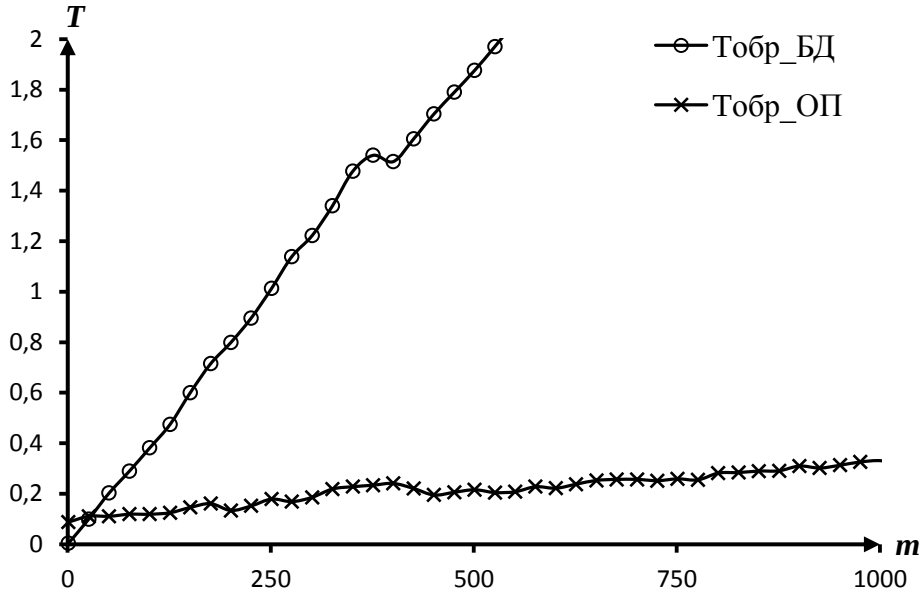


Рисунок 4.1. Зависимость скорости реакции от объема хранимой информации в БД и ОП

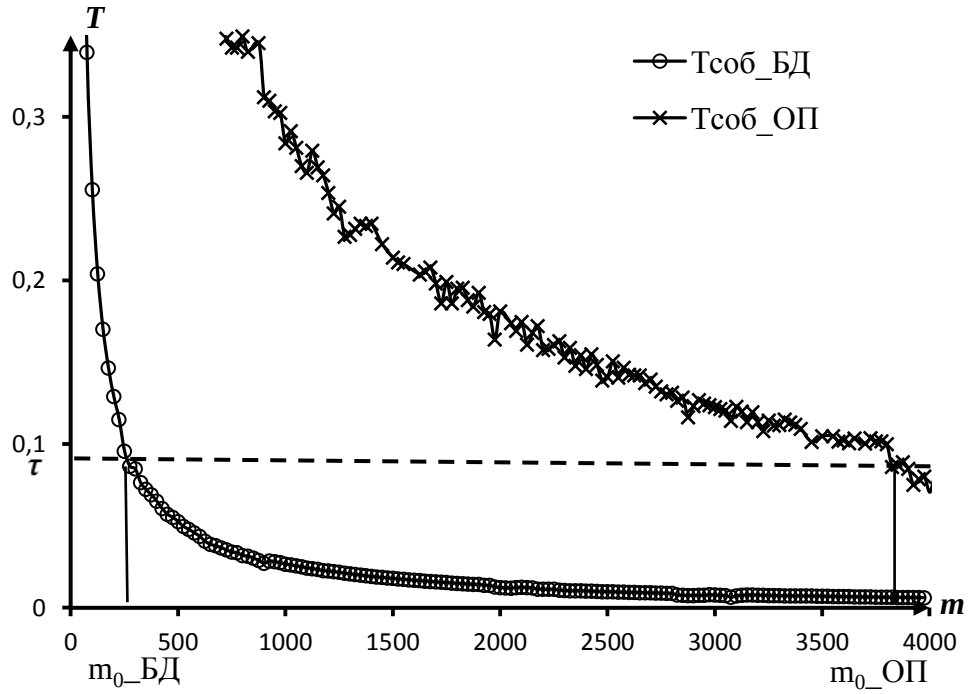


Рисунок 4.2. Зависимость ОРС от объема хранимой информации в БД и ОП

Из анализа графиков (рисунки 4.1, 4.2) следует, что при использовании в качестве хранилища ОП время распознавания существенно ниже, чем при использовании БД.

В соответствии с вышеизложенными условиями в результате эксперимента НПЭФ (τ) составил 0,08, при использовании БД ВПЧЗ (m_0) составил 251, а в случае ОП – 3776 изображений.

Дальнейшие экспериментальные проверки предложенной модели управления безопасностью проводились в офисном здании, оборудованном ИАС. Был получен набор, состоящий из 332 изображений лиц сотрудников. На всех фотографиях положение лица было фронтальное или почти фронтальное. Данное допущение уместно по той причине, что при постановке задачи поиска по фотографии, наиболее вероятно будет использоваться фотография с документов, удостоверяющих личность.

На первом этапе проверялась ИАС в течение часа без применения разработанной модели управления безопасностью.

На втором этапе проверялась ИАС в течение часа с использованием разработанной модели на основании сформированной БД кластеров и разбиения сети видеоконтроля в объединение непересекающихся групп камер и построения вероятностного графа маршрутов.

В ходе экспериментальной проверки определено следующее: целесообразно в начале процесса распознавания сравнивать ключевые признаки интересанта с 10 изображениями лиц с камер вероятность видеофиксации интересанта, на которых выше 0,5 остальных в соответствии с ростом вероятности, а затем с центрами кластеров.

Остановимся на скорости и точности распознавания. Использование разработанной модели позволило повысить точность в среднем на 4,68% и скорость распознавания лиц в среднем на 5,27% (таблица 4.1). Отметим, что в работе [87] точность распознавания достигала 95,01.

Таблица 4.1-Сравнительный анализ эффективности предложенной модели

	ИАС без применения разработанной модели	ИАС с применением разработанной модели
Количество проверяемых изображений	938	1047
Количество успешно распознанных изображений	877	1031
Точность распознавания	93,49	98,18
Среднее время распознавания	0,398	0,377

Согласно рекомендациям Минстроя России по проектированию вокзалов пропускная способность среднего железнодорожного вокзала составляет от 200 до 700 пассажиров в час [37]. Поэтому при указанных характеристиках рассматриваемая ИАС даже с одним ЯИ может функционировать в режиме реального времени на небольшом или среднем железнодорожном вокзале. Отметим, что при использовании более мощного аппаратного обеспечения или с использованием нескольких ЯИ и ЛБД, пропускная способность ИАС увеличиться.

Как и во всех разрабатываемых ранее системах распознавания в экспериментальном ПО, разработанном для проверки выводов настоящего исследования, показано, что время поиска мест пребывания интересанта по изображению его лица определяется следующими составляющими:

- временем извлечения ключевых признаков входного изображения;
- временем их сравнения с центрами кластеров;
- временем извлечения информации из БД по указанному идентификатору.

В результате проведенных тестов установлено, что скорость решения различных аналитических задач по поиску мест видеофиксации интересантов с использованием разработанных структур ЛБД и ЦБД на указанном выше объеме тестируемых данных в среднем занимала 3-4 секунды. Отметим, что данный показатель сильно зависит от количества записей в ЦБД и ЛБД.

Решение аналитической задачи поиска попутчиков интересантов можно рассматривать как определение мест их видеофиксации с учетом их пересечения с множеством зафиксированных ранее в БД лиц в этих же местах за указанный промежуток времени. В результате оператору будет предоставлен список попутчиков с убыванием по частоте видеофиксации с интересантом.

В целях практического определения скорости работы по данному направлению в рамках тестов использовался 5 секундный интервал между видеофиксацией интересанта и его возможных попутчиков. В результате проведенных тестов было установлено, что при наполнении ЛБД и ЦБД 357

лицами скорость решения данной задачи была сопоставима со скоростью определения мест видеофиксации, и составляла в среднем 4-6 секунд.

Далее произведена оценка оптимальности управленческих решений. Для этого:

1. Сформированы две группы руководителей: контрольная и экспертная. Данные группы одинаковы по численности и примерно равны по компетентности.

2. Проведен опрос групп. Каждой группе предлагалось определить план действий при в пятидесяти деструктивных ситуациях. При этом руководители в контрольной группе принимали решения с учетом возможности использования ИАС, а руководители в экспертной группы – без использования ИАС.

3. Полученные решения сравнивались с эталонными решениями, в результате чего определялась их правильность. Также сравнивалось время принятие решений в группах.

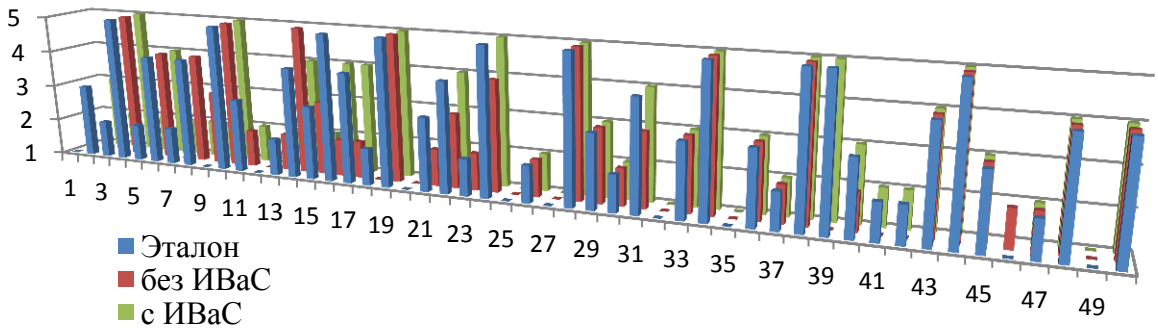


Рисунок 4.3 Результаты оценки определения плана действий по задержанию нарушителя

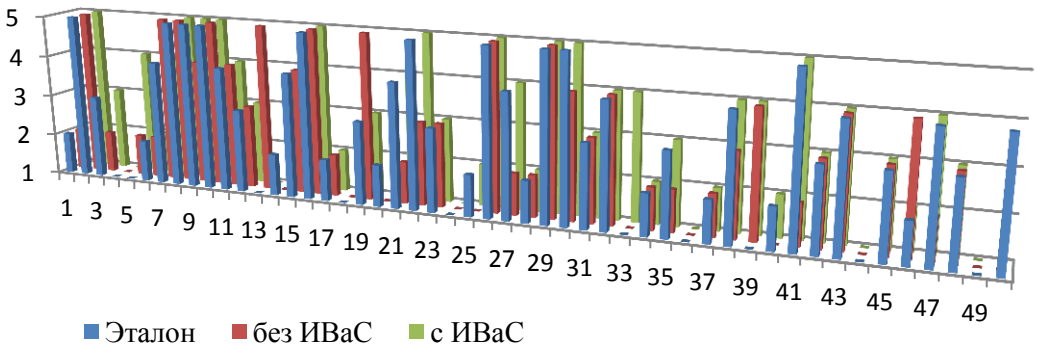


Рисунок 4.4 Результаты оценки определения плана действий по выявлению сообщников

Таблица 4.2 - Результаты экспертного опроса руководителей при определении плана действий

№ ситуации	Оценка						№ ситуации	Оценка					
	Эталон		без ИАС		с ИАС			Эталон		без ИАС		с ИАС	
	№1	№2	№1	№2	№1	№2		№1	№2	№1	№2	№1	№2
1	1	2	1	2	1	1	26	2	5	2	5	2	5
2	3	5	1	5	3	5	27	1	4	1	2	1	4
3	2	3	1	2	2	3	28	5	2	5	2	5	2
4	5	1	5	1	5	1	29	3	5	3	5	3	5
5	2	1	1	2	2	4	30	2	5	2	4	2	5
6	4	2	4	2	4	2	31	4	3	3	3	4	3
7	2	4	1	5	2	4	32	1	4	1	4	1	4
8	4	5	4	5	2	5	33	3	1	3	1	3	4
9	1	5	3	4	2	5	34	5	2	5	2	5	2
10	5	5	5	5	5	5	35	1	3	1	2	1	3
11	3	4	2	4	2	4	36	3	1	3	1	3	1
12	1	3	1	3	1	3	37	2	2	2	2	2	2
13	2	1	2	5	2	1	38	5	4	5	3	5	4
14	4	2	5	1	4	2	39	5	1	1	4	5	4
15	3	4	3	4	2	4	40	3	2	2	1	3	2
16	5	5	2	5	4	5	41	2	5	1	2	2	5
17	4	2	2	2	4	2	42	2	3	1	3	2	3
18	2	1	1	1	2	1	43	4	4	4	4	4	4
19	5	3	5	5	5	3	44	5	1	5	1	5	1
20	1	2	1	1	1	2	45	3	3	3	3	3	3
21	3	4	2	2	3	4	46	1	2	2	4	1	2
22	4	5	3	3	4	5	47	2	4	2	2	2	4
23	2	3	2	3	1	3	48	4	3	4	3	4	3
24	5	1	4	1	5	1	49	1	1	1	1	1	1
25	1	2	1	1	1	2	50	4	4	4	1	4	1

Таблица 4.3 - Результаты оценки временных затрат на определение плана действий

№ ситуации	$t_{без\ ИАС}$, с		$t_{с\ ИАС}$, с		№ ситуации	$t_{без\ ИАС}$, с		$t_{с\ ИАС}$, с	
	№1	№2	№1	№2		№1	№2	№1	№2
1	90	125	80	97	26	8	85	10	64
2	60	56	60	43	27	80	165	50	100
3	53	78	56	15	28	45	75	30	53
4	48	135	20	53	29	70	83	50	82
5	120	146	98	64	30	40	49	25	50
6	40	65	10	12	31	70	89	50	82
7	210	78	150	86	32	47	74	84	25
8	50	25	43	29	33	96	85	50	43
9	120	96	150	45	34	88	78	43	86
10	45	87	57	72	35	120	68	50	15
11	56	103	89	55	36	170	150	43	25
12	70	56	80	48	37	85	86	96	46
13	130	35	50	10	38	156	149	40	26
14	45	78	7	75	39	123	96	140	75
15	25	59	41	54	40	178	82	56	45
16	78	85	70	68	41	456	165	120	36
17	50	46	40	25	42	70	185	30	28
18	12	20	10	15	43	50	145	20	15
19	62	76	43	75	44	180	192	75	85
20	54	58	25	40	45	84	163	73	73
21	70	63	80	15	46	25	146	13	64
22	90	100	85	58	47	10	265	50	46
23	10	52	10	42	48	80	148	10	78
24	5	16	7	20	49	50	82	65	56
25	82	96	74	70	50	84	49	49	15

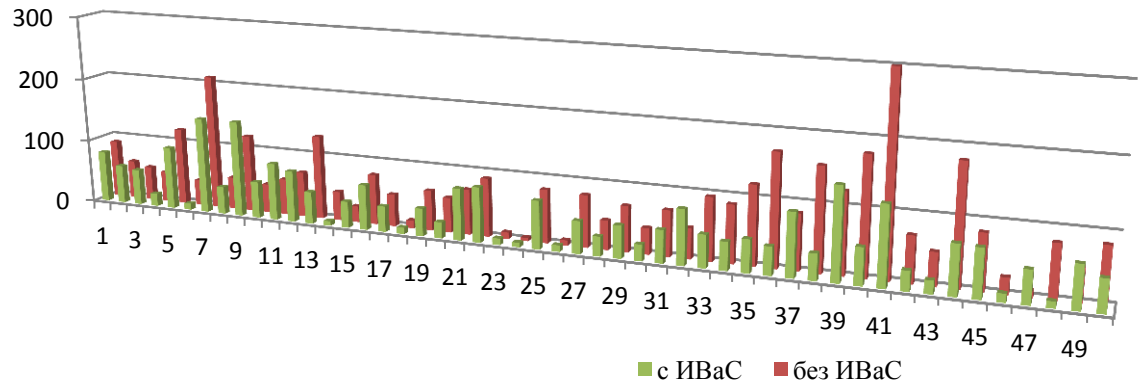


Рисунок 4.5 Результаты оценки временных затрат на определение плана действий по задержанию нарушителя

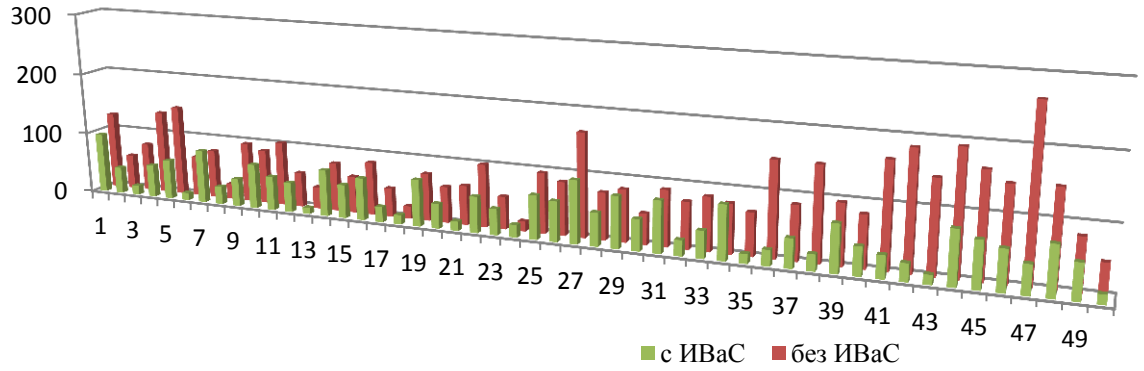


Рисунок 4.6 Результаты оценки временных затрат на определение плана действий по выявлению сообщников

На основе анализа результатов получено:

1) вероятность определения наилучшего плана действий по задержанию нарушителя без использования ИАС составляет 62%, а с использованием – 88%. Следовательно, рост эффективности принятия решений с учетом использования ИАС составляет 26%. Время на принятие решений при использовании ИАС сократилось на 33%.

2) вероятность определения наилучшего плана действий по выявлению сообщников без использования ИАС составляет 58%, а с использованием – 90%. Рост эффективности принятия решений с учетом использования ИАС составляет 32%. Время на принятие решений при использовании ИАС сократилось на 48%.

Таким образом, в среднем рост эффективности принятия решения составляет 29 %, а время на принятие решений в среднем сократилось на 40,5 %.

4.2 Управление персоналом с учетом индивидуальных особенностей

К настоящему времени в мире выполнено большое количество исследований в области управления персоналом. Так одной из самых важных задач в управлении персоналом является определение степени пригодности кандидата на работу. Как правило, решение данной задачи заключается в получении, например посредством анкетирования, эмпирических данных, представляющих характеристики кандидата для дальнейшего их сравнении с эталонными значениями.

По причине того, что в данной работе рассматриваются и предлагаются новые информационные технологии, необходимо, с учетом их специфики, определить эталонные значения характеристик сотрудников, которые позволят им на высоком уровне выполнять работу. При этом необходимо учитывать как профессиональные качества, так и личностные факторы и особенности свойств сенсорной системы. Далее будут определяться требования к сотрудникам на примере оператора ИАС, работа которого в основном связна с аналитической обработкой персональных данных, зрительным анализом человеческих лиц. При этом сотрудник должен выполнять работу как в нормальных условиях, так и при чрезвычайных ситуациях и террористических актах.

В области профессиональных качеств предъявляются стандартные требования IT-специальностей, в частности наличие высшего технического образования, знание основ систем управления базами данных, основ языков программирования и системного администрирования т.д.

Остановимся более подробно на психологических качествах. Для определения эталонных значений параметров характера сотрудника будем использовать типохарактерную классификацию [48] (таблица 4.4).

Таблица 4.4 – Типохарактерная классификация с учетом общих характеристик

Черта характера	**Характеристики**
экстравертная (E)	общительность, мощное расходование энергии, обширные связи
интровертная (I)	задумчивость, сосредоточенность, иногда замкнутость, сохранение внутренней энергии
сенсорная (S)	практичность, конкретность, хорошая память на зрительные и слуховые образы, трудность в установлении причинно-следственных связей
интуитивная (N)	размытое восприятие зрительных и слуховых образов, оригинальность в решении задач, высокая способность в выявлении причинно-следственных связей
думающая (T)	объективность, твердость характера, использование аналитических методов при решении задач
чувствующая (F)	чуткость, гуманность, гармоничность, мягкосердечность
решающая (J)	выполняет работу вовремя, рабочий день четко спланирован, во всем любит определенность, работает ритмично
воспринимающая (P)	выполняет работу к самому крайнему сроку, не любит ритмичную работу, способен оценить импровизацию, любит неожиданности и сюрпризы, предпочитает случайный компонент информации

Исходя из существующих представлений соционики, индивид может обладать только одним типом характера из 16 возможных: ESTJ, ESTP, ESFJ, ESFP, ENTJ, ENTP, ENFJ, ENFP, ISTJ, ISTP, ISFJ, ISFP, INTJ, INTP, INFJ, INFP.

На основе работ [42], [40] рассмотрим некоторые особенности сенсорной видеосистемы у индивидуумов с определенной доминантой в характере и зададим предпочтение доминанты к работе с ИАС (таблица 4.5).

Таблица 4.5 – Типохарактерная классификация с учетом особенностей сенсорной видеосистемы

Доминанта	**Особенности сенсорной видеосистемы**	**Вес доминанты**
экстравертная (E)	хорошо распознают текстуру изображения	1
интровертная (I)	хорошо распознают контуры, неразговорчивы	2,5
сенсорная (S)	время реакции короче, острота зрения выше, чем у интуитивной доминанты, хорошо запоминают мелкие детали	3,5
интуитивная (N)	оригинальность в решении задач	1
думающая (T)	характерно восприятие зрительного образа в широком динамическом диапазоне	1,5
чувствующая (F)	панорамное широкомасштабное восприятие, обладают хорошей памятью на лица	3
решающая (J)	аккуратность, средняя частота ошибок ниже, чем у воспринимающей доминанты	3,3
воспринимающая (P)	быстрота, внимательность к нюансам	2

Таким образом, распределение предпочтений по доминантам представлено на рисунке 4.7.

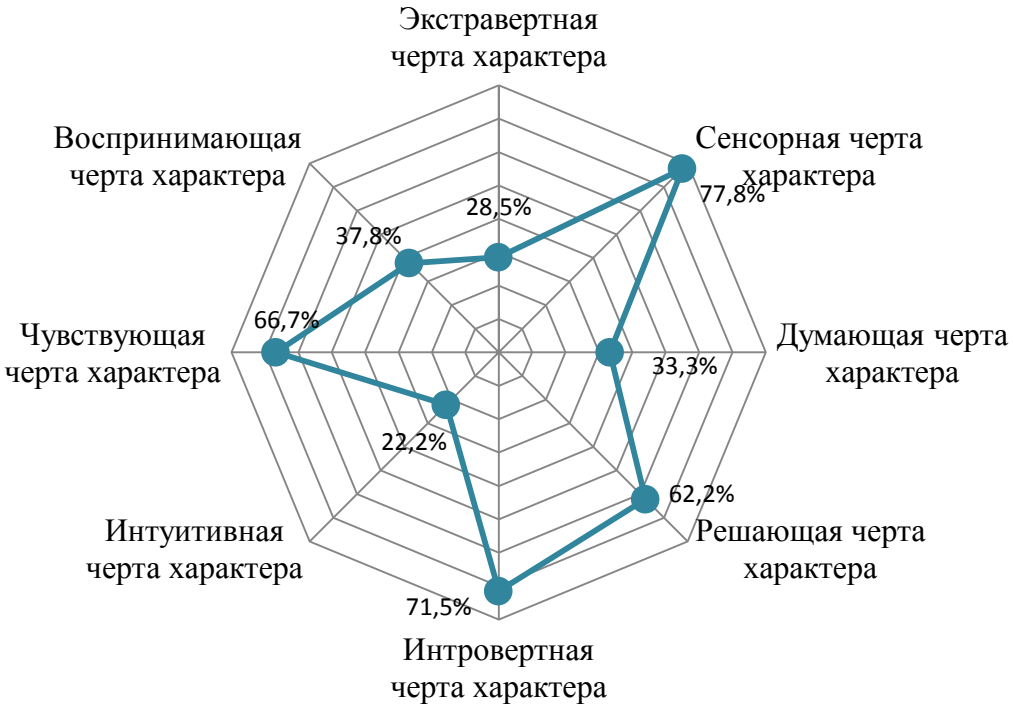


Рисунок 4.7. Распределение предпочтений по видео-сенсорным системам индивида

Поскольку работа оператора связана с доступом к персональным данным, с целью минимизации рисков, например коррупционного характера, рекомендуется набирать сотрудников, которые находятся на достаточно высокой ступени в пирамиде Маслоу [34] (рисунок 4.8).

Рисунок 4.8. Нижний порог социального уровня

4.3 Экономический эффект

Экономический эффект от внедрения разработанной ИАС будет выражаться в снижении материального ущерба, связанного с деструктивными действиями нарушителя, в частности террористическими актами и пожарами.

Рассмотрим ущерб от террористических актов. По данным отчета Института экономики и мира [108] в 2014 году террористические акты нанесли ущерб мировой экономике в $ 52,9 млрд. Стоит отметить, что размер ущерба примерно равен ВВП Болгарии. При расчете ущерба учитывалась стоимость поврежденного имущества, потери жизни и нанесенных увечий, включая стоимость медицинских страховок и упущенных доходов. В расчеты не включалась стоимость, затраченная на увеличение количества правоохранителей.

По информации, отраженной в данном отчете террористическая группировка «Исламское государство» (запрещена на территории РФ) за 2014 год убила 20 000 человек. Кроме того, составлен рейтинг стран наиболее подверженных террористической угрозе. Россия заняла 23-е место с «красным» уровнем угрозы.

Для оценки экономического ущерба от 1-го теракта ($s_т$) в России оценим средний ущерб в мире. Согласно таблице атак и смертей в России и странах СНГ совершено 450 террористических актов, в которых погибло 724 человека. Отметим, что в результате 1-го теракта погибает в среднем 1, 6 человека. Средний экономический ущерб от теракта может быть вычислен следующим образом ($s_т$):

$$s_т = \frac{s^т{}_{общ}}{\sum_i k^т{}_i}, \tag{4.1}$$

где

- $s_т$ – средний экономический ущерб от теракта;
- $s^т{}_{общ}$– экономический ущерб от терактов ($s_{общ}$ = \$52,9 млрд);
- $k^т{}_i$ – количество терактов в регионе;
- i – индекс региона.

Подставляя в формулу (4.1) приведенные на рисунок 4.9 значения параметров, получаем следующее: средний экономический ущерб от 1-го теракта

в мире составляет $s_т = $3,96 млн. Без ограничения общности будем считать, что ущерб от 1-го теракта в мире сопоставим с ущербом от 1-го теракта в России.

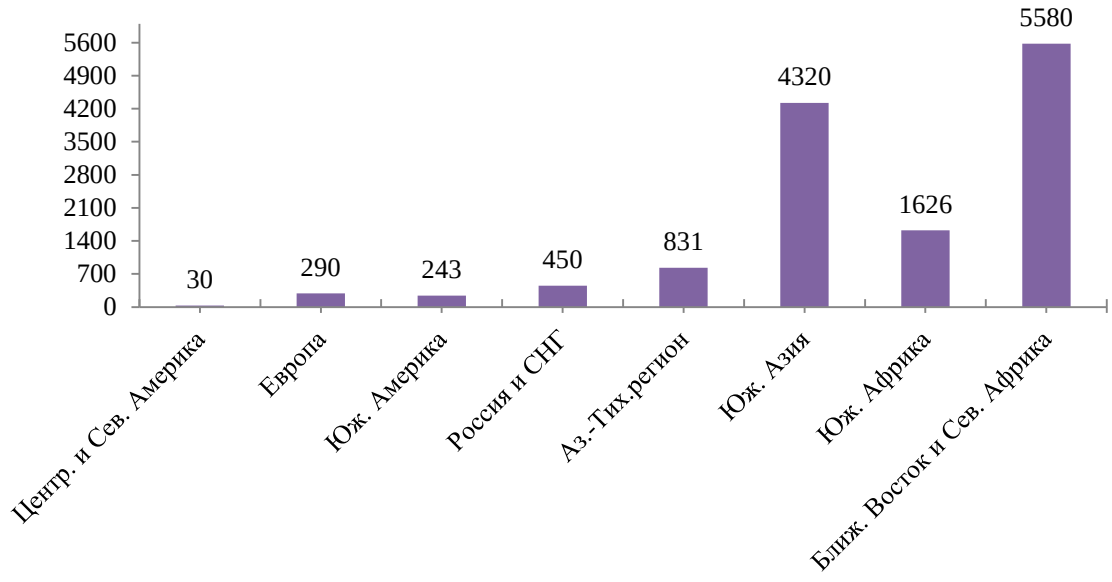


Рисунок 4.9. Количество терактов в мире по регионам

Так же обратим внимание на пожары и на основе статистического сборника [52] оценим ущерб от пожаров в местах массового пребывания людей (общественных местах). Так общее количество пожаров ($k^{п}_{общ}$) в 2015 году составило 145,9 тыс., прямой материальный ущерб ($s^{п}_{общ}$) – 22 461 847 тыс. руб., прямой материальный ущерб от 1-го пожара – 153 909,4 руб. Для оценки среднего материального ущерба от 1-го пожара в общественных местах будем рассматривать следующие объекты:

1) здания, сооружения и помещения предприятий торговли;
2) здания учебно-воспитательного назначения;
3) здания здравоохранения и социального обслуживания населения;
4) здания, помещения сервисного обслуживания населения;
5) административные здания;
6) здания, сооружения и помещения для культурно-досуговой деятельности населения и религиозных обрядов;
7) прочие здания, сооружения и помещения общественного назначения.

Таким образом, средний экономический ущерб от 1-го пожара на общественном объекте может быть вычислен следующим образом ($s_п$):

$$s_{\text{п}} = \frac{s^{\text{п}}{}_{\text{общ}} \sum_i s^{\text{п}}{}_i}{k^{\text{п}}{}_{\text{общ}} \sum_i k^{\text{п}}{}_i}, \quad (4.2)$$

где

- $s_{\text{п}}$ – средний экономический ущерб от 1-го пожара в общественном объекте;
- $s^{\text{п}}{}_{\text{общ}}$ – экономический ущерб от всех пожаров на общественных объектах ($s^{\text{п}}{}_{\text{общ}} = 22\,461\,847$ тыс. руб.);
- $s^{\text{п}}{}_i$ – экономический ущерб от пожара на i-ах общественных объектах от общего экономического ущерба;
- $k^{\text{п}}{}_{\text{общ}}$– общее количество пожаров ($k^{\text{п}}{}_{\text{общ}} = 145{,}9$ тыс);
- $k^{\text{п}}{}_i$ – количество пожаров на i-ах общественных объектах от общего количества пожаров;
- i – индекс объекта общественного назначения, $i \in \{1 \dots 7\}$.

Подставляя в выражение (4.2) приведенные значения параметров, получаем: средний экономический ущерб от 1-го пожара составляет $s_{\text{п}} = 619\,630$ руб.

Отметим, что в 2015 г. в результате пожаров в общественных объектах погибло 87 людей.

Проанализировав статистику, представленную в таблица 4.6, можно сделать следующий вывод: количество пожаров на общественных объектах составляет 4,01% от общего количества пожаров, но материальный ущерб от них – 16,14%. Следовательно, данные объекты в значительно меньшей степени подвержены пожарам, но пожар наносит более существенный ущерб. Средний материальный ущерб от 1-го пожара на общественном объекте составляет 619 630 руб., что существенно выше среднестатистического материального ущерба от 1-го пожара во всех типах сооружений (153 909,4 руб.).

Предположим, что комплекс технических средств ИАС позволит обеспечить противопожарную и антитеррористическую защиту новых общественных объектов, а именно зданий социального, культурного и бытового назначения.

Таблица 4.6 – Распределение основных показателей обстановки с пожарами в РФ за 2011-2015 гг.

Объект пожара	Количество пожаров, ед. / % от общего количества пожаров Прямой материальный ущерб, тыс. руб. / % от общего ущерба Погибло, чел. / % от общего количества погибших									
	2011		2012		2013		2014		2015	
1	2	3	4	5	6	7	8	9	10	11
Здания производственного назначения	3814	2,26	3459	2,12	3137	2,04	3099	2,05	2930	2,01
	2212136	12,16	2337422	14,89	924216	6,21	1244516	6,82	2868191	12,77
	159	1,32	142	1,22	95	0,90	113	1,11	95	1,01
Складские здания, сооружения	1541	0,91	1463	0,90	1422	0,93	1395	0,93	1306	0,89
	5443539	29,91	2289232	14,59	3273889	21,99	3833640	21,01	5155743	22,95
	58	0,48	33	0,28	21	0,20	14	0,14	15	0,16
Здания, сооружения и помещения предприятии торговли	4081	2,42	3831	2,35	3568	2,32	3212	2,13	3037	2,08
	1340938	7,37	1523165	9,71	2206907	14,83	2371965	13,00	2718646	12,10
	29	0,24	17	0,15	18	0,17	16	0,16	32	0,34
Здания учебно-воспитательного назначения	348	0,21	333	0,20	270	0,18	228	0,15	290	0,20
	25023	0,14	59617	0,38	39023	0,26	56337	0,31	125222	0,56
	3	0,02	1	0,01	4	0,04	1	0,01	2	0,02
Здание здравоохранения и социального обслуживания населения	251	0,15	217	0,13	223	0,15	192	0,13	171	0,12
	22574	0,12	29821	0,19	39202	0,26	34741	0,19	29401	0,13
	7	0,06	3	0,03	83	0,78	9	0,09	26	0,28
Здания, помещения сервисного обслуживания населения	835	0,50	1026	0,63	1057	0,69	1090	0,72	1037	0,71
	333403	1,83	242285	1,54	187611	1,26	275613	1,51	252962	1,13
	11	0,09	11	0,09	7	0,07	7	0,07	11	0,12
Административные здания	1101	0,65	969	0,59	938	0,61	880	0,58	910	0,62
	201333	1,11	478283	3,05	189756	1,27	408119	2,24	352566	1,57
	18	0,15	12	0,10	14	0,13	20	0,20	13	0,14
Здания, сооруж. и помещ. для культурно-досуговой деят. населения и религ. обрядов	376	0,22	323	0,20	305	0,20	266	0,18	262	0,18
	40713	0,22	99333	0,63	54747	0,37	83035	0,46	95714	0,43
	5	0,04	1	0,01	1	0,01	1	0,01	1	0,01
Здания для временного пребывания (проживания) людей	432	0,26	300	0,18	258	0,17	211	0,14	248	0,17
	60193	0,33	709599	4,52	36807	0,25	53630	0,29	296616	1,32
	46	0,38	26	0,22	20	0,19	15	0,15	17	0,18
Здания жилого назначения и надворные постройки	119345	70,82	113251	69,51	104592	68,15	103579	68,68	100498	68,86
	5474098	30,08	4933670	31,44	4450833	29,90	5214726	28,58	4939457	21,99
	11050	91,94	10740	92,17	9670	91,12	9339	92,12	8515	90,54
в т.ч. жилой дом	66935	39,72	64205	39,41	58867	38,36	57724	38,28	55132	37,78
	3480794	19,13	3025181	19,28	2880661	19,35	3323648	18,22	3135179	13,96
	9407	78,27	9167	78,67	8244	77,69	7869	77,62	7065	75,12
Здания и сооружения сельскохозяйственного назначения	776	0,46	680	0,42	694	0,45	617	0,41	552	0,38
	204383	1,12	316727	2,02	483056	3,25	593424	3,25	2129714	9,48
	24	0,20	22	0,19	22	0,21	14	0,14	8	0,09
Место открытого хран. веществ, материалов, с/х угодья и прочие открытые территории	3228	1,92	3738	2,29	3443	2,24	3511	2,33	4098	2,81
	235102	1,29	173446	1,11	89635	0,60	260347	1,43	186734	0,83
	15	0,12	19	0,16	8	0,08	10	0,10	16	0,17
Сооружения, установки промышленного назначения	1145	0,68	1095	0,67	1098	0,72	927	0,61	896	0,61
	162654	0,89	201289	1,28	236681	1,59	1202446	6,59	314255	1,40
	64	0,53	62	0,53	63	0,59	57	0,56	38	0,40
Строящееся (реконструируемые) здания (сооружения)	1002	0,59	952	0,58	978	0,64	976	0,65	977	0,67
	239666	1,32	101873	0,65	283359	1,90	158916	0,87	153099	0,68
	52	0,43	38	0,33	38	0,36	29	0,29	40	0,43
Прочие здания, сооружения и помещения общественного назначения**	221	0,13	166	0,10	165	0,11	151	0,10	141	0,10
	17454	0,10	47279	0,30	10521	0,07	55405	0,30	49086	0,22
	8	0,07	6	0,05	4	0,04	5	0,05	2	0,02
Отдельно стоящая хозяйственная постройка (бытовка, вагончик, сарай, хозблок, будка и др.)*	0	0,00	1153	0,71	1456	0,95	1766	1,17	1859	1,27
	0	0,00	21598	0,14	20792	0,14	29093	0,16	25090	0,11
	0	0,00	106	0,91	134	1,26	134	1,32	138	1,47
Неэксплуатируемое здание (сооружение)	2531	1,50	2328	1,43	2763	1,80	2788	1,85	3373	2,31
	70733	0,39	56125	0,36	68464	0,46	83526	0,46	79125	0,35
	169	1,41	135	1,16	148	1,39	145	1,43	160	1,70
Транспортные средства	23401	13,89	24266	14,89	23434	15,27	22847	15,15	20817	14,26
	1984578	10,91	2035426	12,97	2259733	15,18	2246966	12,31	2414480	10,75
	135	1,12	145	1,24	158	1,49	123	1,21	157	1,67
Прочие объекты пожара	1926	1,14	1605	0,99	1837	1,20	1326	0,88	785	0,54
	129166	0,71	36328	0,23	29688	0,20	39966	0,22	275498	1,23
	59	0,49	48	0,41	29	0,27	28	0,28	36	0,38
Носильные вещи (вещи на человеке)	2174	1,29	1764	1,08	1828	1,19	1742	1,16	1755	1,20
	610	0,00	874	0,01	419	0,00	153	0,00	247	0,00
	107	0,89	85	0,73	75	0,71	58	0,57	83	0,88

Воспользуемся статистическими сборниками [73], [72], [75], [74] для определения количества новых зданий социального, культурного и бытового назначения с 2011 по 2015 года (рисунок 4.10). Так за указанный период было построено 64 825 зданий указанного типа. Будем считать, что количество построенных зданий в период 2016-2021 годов будет аналогичным и составит 64 825 (n).

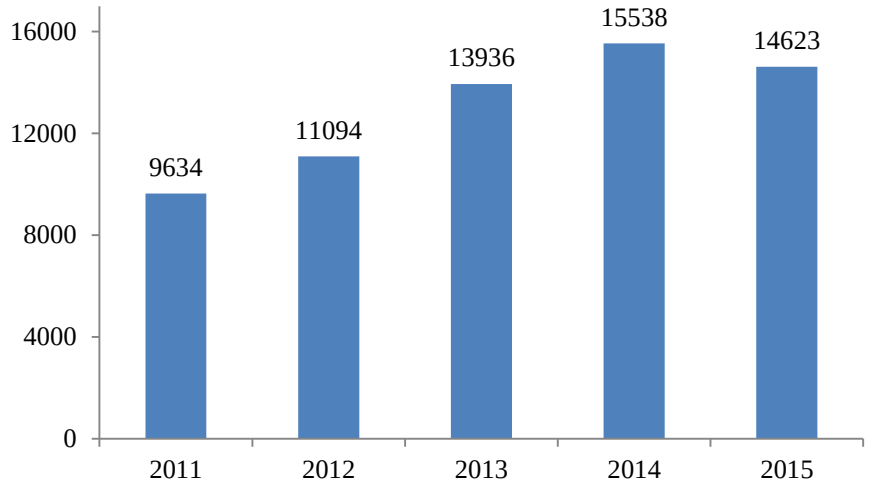


Рисунок 4.10. Ввод в действие зданий системы здравоохранения, коммерческих, административных, учебных и других общественных домов

Вероятность пожара на общественных объектах можно вычислить на основе данных из статьи [14] (таблица 4.7). Просуммировав значения столбца с частотой возникновения пожара и разделив на количество учреждений, можно определить частоту возникновения пожара на общественном объекте ($p_{\text{п}}$). Таким образом, $p_{\text{п}}$ = 2,716 *10^{-3}.

Таблица 4.7 – Частота возникновения пожара для общественных зданий

№	Наименование общественного учреждения	Частота возникновения пожара в течение года
1.	Дошкольные	$7{,}34 \cdot 10^{-3}$
2.	Общеобразовательные	$1{,}16 \cdot 10^{-2}$
3.	Начального профессионального образования	$1{,}98 \cdot 10^{-2}$
4.	Среднего профессионального образования	$2{,}69 \cdot 10^{-2}$
5.	Высшего профессионального образования	$1{,}398 \cdot 10^{-1}$
6.	Прочие внешкольные и детские учреждения	$1{,}52 \cdot 10^{-2}$
7.	Детские оздоровительные лагеря, летние детские дачи	$1{,}26 \cdot 10^{-3}$
8.	Больницы, госпитали, клиники, родильные дома,	$3{,}66 \cdot 10^{-2}$

	психоневрологические интернаты и другие стационары	
9.	Санатории, дома отдыха, профилактории, дома престарелых и инвалидов	$2{,}99 \cdot 10^{-2}$
10.	Амбулатории, поликлиники, диспансеры, медпункты, консультации	$8{,}88 \cdot 10^{-3}$
11.	Предприятия розничной торговли	$2{,}03 \cdot 10^{-2}$
12.	Предприятия рыночной торговли	$1{,}13 \cdot 10^{-2}$
13.	Предприятия общественного питания	$3{,}88 \cdot 10^{-2}$
14.	Гостиницы, мотели	$2{,}81 \cdot 10^{-2}$
15.	Спортивные сооружения	$1{,}83 \cdot 10^{-3}$
16.	Клубные и культурно-зрелищные учреждения	$6{,}90 \cdot 10^{-3}$
17.	Библиотеки	$1{,}16 \cdot 10^{-3}$
18.	Музеи	$1{,}38 \cdot 10^{-2}$
19.	Зрелищные учреждения (театры, цирки)	$9{,}66 \cdot 10^{-2}$

По официальным данным [73] в России в 2015 году совершено 8 терактов, а количество общественных объектов около 262 147. Предположим, что целью террористов является создание наибольшего резонанса в обществе и убийство максимального количества людей, тогда коэффициент террористических угроз общественному зданию ($p_{\text{т}}$) равняется делению количества терактов на количество общественных объектов, таким образом, $p_{\text{т}} = 3{,}05 * 10^{-5}$.

Далее оценим стоимость ИАС без учета стоимости разработанной в данной работе ПО. Так стоимость оборудования и монтажа ИАС (c_1), состоящего из 32-ух ip-камер, сервера с модулем детектирования, сервера с ядром идентификации, сервера кластеризации, сервера запросов, аналитического модуля, сервера приложений и 4-х автоматизированных рабочих мест составит примерно 2 559 678 руб. (c_1). Ежегодные затраты на техническое сопровождение оборудования составляют около 57 000 руб. (c_2). При этом предполагается, что на объекте присутствует охрана и не требуется дополнительных затрат на ее обучение пользованием ИАС.

Тогда за первый год внедрения ИАС экономический эффект составит:

$$E_1 = E^{\text{т}}{}_1 + E^{\text{п}}{}_1 = \frac{n}{t} * (p_{\text{т}} s_{\text{т}} + p_{\text{п}} s_{\text{п}} - (p_{\text{т}} + p_{\text{п}}) * \sum_i c_i), \quad (4.3)$$

где:

- $E^{т}{}_{1}$ – экономический эффект с учетом обеспечения антитеррористической безопасности;
- $E^{п}{}_{1}$ – экономический эффект с учетом обеспечения противопожарной безопасности;
- n – количество построенных общественных зданий за 5 лет (n = 64 825);
- t – анализируемый временной промежуток (t = 5 лет);
- $p_{т}$– коэффициент террористических угроз ($p_{т} = 3{,}05 * 10^{-5}$);
- $p_{п}$– коэффициент угроз пожарного характера ($p_{п}$ = 2,716 $*10^{-3}$);
- $s_{п}$ – средний экономический ущерб от 1-го пожара в общественном месте ($s_{п} = 382\,499{,}62$ руб.);
- $s_{т}$ – средний экономический ущерб от теракта (будем считать \$1 = 60 руб., тогда $s_{т} = 3{,}96 * 10^{6} * 60 = 237{,}6 * 10^{6}$ руб.);
- c_1 – затраты на установку ИАС ($c_1 = 2\,559\,678$ руб.);
- c_2 – ежегодные затраты на техническое сопровождение ИАС ($c_2 = 57\,000$ руб.).

Получаем: экономический эффект E_1 = 22 606 тыс. руб. в первый год внедрения ИАС на новых общественных объектах.

Поскольку в последующие годы рассматриваемого периода не потребуется закупка оборудования и его монтаж, экономический эффект со 2 по 5 года составит:

$$E_{2-5} = t_{исп} * \frac{n}{t} * (p_{т}s_{т} + p_{п}s_{п} - (p_{т} + p_{п}) * c_2), \quad (4.4)$$

где $t_{исп}$ – число рассматриваемых лет использования ИАС после внедрения ($t_{исп} = 4$).

Подставив значения, получаем экономический эффект от внедрения ИАС за 4 года составит E_{2-5} = 455 165 тыс. руб.

В результате, просуммировав значения выражений (4.3) и (4.4) получаем, что экономический эффект от внедрения ИАС за 5 лет составит 477 771 тыс. руб.

4.4 Вывод по четвертой главе

В данной части исследования были представлены практические результаты применения разработанных в исследовании моделей и алгоритмов.

Практически реализованный в тестовом режиме один из вариантов ПО ИАС на основе сделанных выше выводов о ее моделях и алгоритмах показал следующее: ИАС при ее реализации в данном виде позволяет работать в режиме «реального времени». Точность распознавания составила 98,18 % (увеличение на 4,68%), а время распознавания 0,377 с. (сокращение на 5,27%) на изображениях, сделанных в промежутке от года до четырех лет, что лучше, чем у аналогичных, предложенных ранее систем. В рамках реализации ПО экспериментальной ИАС установлено, что она в состоянии решать аналитические задачи по поиску мест видеофиксации интересантов в среднем за 3-4 с., и поиску попутчиков интересантов в среднем за 4-6 с.

Выявлен рост показателей результативности управленческих решений, принимаемых с учетом использования предлагаемой ИАС: повышение точности и правильности решений при выборе оптимального плана мероприятий на 29% и сокращение времени на принятие решения в среднем на 40,5%.

Кроме того, разработаны рекомендации по определению степени пригодности кандидата к работе в службе безопасности с учетом индивидуальных особенностей. При этом учитывались как профессиональные качества, так и личностные факторы и особенности свойств сенсорной системы. Рекомендации определялись на примере оператора ИАС, работа которого в основном связана с аналитической обработкой персональных данных, зрительным анализом человеческих лиц. При этом учитывалось, что сотрудник должен выполнять работу как в нормальных условиях, так и при чрезвычайных ситуациях и террористических актах.

На основе разработанной методики проведен расчет предполагаемого экономического эффекта от внедрения ИАС для обеспечения безопасности. суммарный эффект в течение ближайших пяти лет, определяемый снижением количества преступлений и материального ущерба, составит 435 852, 7 тыс. руб.

ЗАКЛЮЧЕНИЕ

Основным научным результатом данной работы являются модель, алгоритм и структура системы информационно-аналитической поддержки управления безопасностью людей в местах их массового пребывания. По итогам диссертационной работы получены следующие результаты:

1. В ходе анализа современного состояния безопасности людей в местах их массового пребывания определено, что защищенность при эффективном и экономном использовании сил и средств может быть повышена за счет использования информационно-аналитической системы на базе идентификации по изображению, которая позволит повысить результативность и оперативность управленческих решений.

Однако в результате анализа выявлена практическая невозможность использования функций подобных существующих решений для комплексной и оперативной поддержки управления в условиях неопределенности информации при неконтролируемой обстановке в местах массового пребывания людей. Отмечается, что в большинстве существующие системы направлены только на информирование об обнаруженном нарушителе, применение же данных технологий для поддержки управления безопасностью людей с учетом особенностей мест их массового пребывания требует новых решений.

Кроме того, выявлены наиболее значимые факторы, и разработана классификация нарушителей, учитывающая уровень потенциала и угрозы безопасности.

2. С целью повышения безопасности людей предложена стохастическая модель информационно-аналитической поддержки управления, позволяющая стабилизировать оборудованные автоматизированными системами идентификации по изображению места их массового пребывания. Предложенная модель, в отличие от существующих, позволяет описать управление безопасностью людей в местах их массового пребывания с учетом индивидуальных особенностей сотрудников службы безопасности, поведения нарушителей и параметров автоматизированной системы идентификации по

изображению. С использованием модели орган управления может получать объективную оценку распределения и поведения нарушителей и координировать силы и средства охраны.

3. На основе разработанной математической модели получена оценка вероятности обнаружения нарушителей в местах массового пребывания людей, учитывающая в комплексе время реакции персонала, неравномерную скорость движения нарушителей, параметры автоматизированной системы идентификации по изображению. С использованием данной оценки могут быть разработаны организационно-технические требования к нормативным значениям времени обнаружения и задержания нарушителя.

4. Для повышения эффективности обнаружения нарушителей разработаны рекомендации по определению степени пригодности кандидата к работе в дежурно-диспетчерской службе с учетом индивидуальных особенностей. При этом учитывались как профессиональные качества, так и личностные факторы и особенности свойств сенсорной системы.

5. Впервые с учетом особенностей автоматизированных систем идентификации по изображению предложен алгоритм поддержки управления безопасностью людей в местах их массового пребывания. Отличительной особенностью данного алгоритма является возможность обоснованного расчета числа и мест дислокаций сотрудников службы безопасности на основе оценки вероятности обнаружения нарушителей и прогнозирования их маршрутов следования с учетом особенностей мест массового пребывания людей.

6. С целью повышения оперативности управленческих решений разработана структура системы на базе идентификации по изображению. В алгоритме функционирования предложенной системы успешно используются впервые полученные зависимости скорости реакции систем данного типа от объема информации в базах данных и нагрузки сети видеоконтроля и усовершенствованный гибридный подход к идентификации на основе уникальности биометрии лица. Данная система способствует обоснованному принятию решений при проведении мероприятий по противодействию

дестабилизациям, в частности при определении числа и мест дислокаций сотрудников службы безопасности, выявлении связей и вероятных мест пребываний нарушителей.

7. Реализованная в тестовом режиме предлагаемая система поддержки управления на базе идентификации по изображению позволила повысить следующие показатели: точность и правильность решений в среднем увеличена на 29%, время принятия решений в среднем сокращено на 40,5%.

8. Проведен расчет предполагаемого экономического эффекта от внедрения данной системы поддержки управления безопасностью людей в местах их массового пребывания. Суммарный эффект в течение ближайших пяти лет, определяемый снижением количества преступлений и материального ущерба, составит 477 771 тыс. руб.

Таким образом, в диссертационной работе представлены новые научно обоснованные решения информационно-аналитической поддержки управления безопасностью людей в местах их массового пребывания. Внедрение данных результатов способствует значительному повышению уровня общественной безопасности на территории Российской Федерации.

СПИСОК СОКРАЩЕНИЙ

Список русскоязычных сокращений

АДС	Архитектура Динамических Связей
АМФ	Активная Модель Формы
АНК	Анализ Независимых Компонент
АРМ	Автоматизированное (-ые) Рабочее(-ие) Место (-а)
БД	База Данных
ВЛДА	Вероятностный Линейный Дискриминантный Анализ
ВПЧЗ	Верхний Порог Числа Записей
ГМ	Гибридный Метод анализа изображения
ГФ	Главный Фактор
ИАС	Информационно-Аналитическая Система
ИЕХ	Информационная Единица Хранения
КГФ	Классификатор Габора-Фишера
ЛБД	Локальная База Данных
ЛБШ	Локальные Бинарные Шаблоны
ЛДА	Линейный Дискриминантный Анализ
МГК	Метод Главных Компонент
МГС	Метод Гибкого Сравнения на графах
МД	Модуль видео Детектирования
ОРС	Относительная Реакция Системы
ОКХГ	Объединение Крупномасштабных Характеристик Габора
ОП	Оперативная Память
ОС	Операционная Система
ПГЛБШГ	Последовательность Гистограмм Локальных Бинарных Шаблонов Габора
ПВГ	Представление Вейвлетом Габора
ПО	Программное Обеспечение

ПОЛ	Потенциально Опасное Лицо
СОБ	Система Обеспечения Безопасности
СУБД	Система Управления Базами Данных
ЦБД	Централизованная База Данных
ЯИ	Ядро Идентификации
ЯП	Язык Программирования

Список англоязычных сокращений

AAM	Active Appearance Models в дословном переводе означает "активные модели внешнего вида" метод распознавания лиц за счёт построения статистических моделей изображений, которые путем разного рода деформаций могут быть подогнаны под реальное изображение
ASM	Active Shape Models в дословном переводе означает "активные модели форм" метод распознавания лиц за счёт учета статистических связей между расположением антропометрических точек на лицах
CCA	Canonical Correlation Analysis в дословном переводе означает "канонический корреляционный анализ"
EEF	Equal Error Rate в дословном переводе означает "уровень равенства ошибок" вероятность того, что FRR равна FAR
FAR	False Acceptance Rate в дословном переводе означает "уровень ложного принятия", ошибка систем детектирования лиц второго рода показывает какая часть лиц из всего видеопотока система распознает, но на самом деле распознанный объект не находится в БД (или

	система путает распознанный объект с другим человеком), или вероятность ложного совпадения биометрических характеристик двух людей
	Failure to Acquire Rate в дословном переводе означает "вероятность отказа сбора данных", ошибка систем детектирования лиц показывает долю попыток верификации или идентификации, для которых система распознавания лиц не может создать биометрический шаблон
FER	Failure to Enroll Rate в дословном переводе означает "уровень отказа в регистрации", вероятность того, что система не сможет зарегистрировать человека
FERET	Face Recognition Technology в дословном переводе означает "технология распознавания лиц", разработанная агентством DARPA и исследовательской лабораторией армии США исследовательская программа для оценки эффективности алгоритмов распознавания лиц
FNR	False Negative Rate в дословном переводе означает "уровень отрицательного распознавания", показывает долю не верно детектированных лиц модулем детектирования
FRR	False Rejection Rate в дословном переводе означает "уровень ложного отказа", ошибка систем детектирования лиц первого рода показывает какая часть лиц из всего видеопотока не будет распознана системой или вероятность отказа доступа человеку, имеющего допуск
ICA	Independent Component Analysis

	в дословном переводе означает "анализ независимых компонент" (АНК)
LBP	Local Binary Pattern в дословном переводе означает "локальный бинарный шаблон" (ЛБШ)
LDA	Linear Discriminant Analysis в дословном переводе означает "линейный дискриминантный анализ" (ЛДА) аббревиатура используется для обозначения метода распознавания изображений с соответствующим названием
LFA	Local Feature Analysis в дословном переводе означает "анализ признаков лица" аббревиатура используется для обозначения метода распознавания изображений с предварительной настройкой алгоритмов распознавания в нейронной сети для определения значимости каждого из локальных признаках лица
LGBPHS	Local Gabor Binary Pattern Histogram Sequence в дословном переводе означает "последовательность гистограмм локального бинарного шаблона Габора" (ПГЛБШГ)
NIST	National Institute of Standards and Technology в дословном переводе означает "Национальный институт стандартов и технологий США"
PCA	Principal Component Analysis в дословном переводе означает "анализ главных компонент" аббревиатура используется для обозначения метода главных компонент (МГК)
POI	Percent Of Identification в дословном переводе означает "процент идентификации"

ЛИТЕРАТУРА

1. Алехин Е.М., Брушлинский Н.Н., Вагнер П., Коломиец Ю.И., Соколов С.В. Проблемно-ориентированные имитационные системы для автоматизированного проектирования и стратегического управления экстренными и аварийно-спасательными службами городов, Вестник российской академии естественных наук. М.: РАЕН. 2012/3
2. Алфимцев А.Н., Демин Н.А. Захват и отслеживание удаленных объектов в видео-потоке //Инженерный журнал: наука и инновации, 2013, вып. 11.
3. Алфимцев А.Н., Лычков И.И., Метод обнаружения объекта в видеопотоке в реальном времени. //Вестник Тамбовского государственного технического университета, 2011, т. 17, № 1, с. 44–55.
4. База данных Color FERET, [Электронный ресурс], режим доступа: http://www.nist.gov/itl/iad/ig/colorferet.cfm.
5. Бедило М.В., Бердашев Б.Ж., Бутузов С.Ю., Своеступов М.В. О проблемах межведомственного управления подразделениями при ликвидации чрезвычайных ситуаций, Интернет-журнал "Технологии техносферной безопасности" (http://ipb.mos.ru/ttb) Выпуск № 3 (49), 2013 г.
6. Более 60% преступлений в московском метро раскрыли при помощи камер, 4 декабря 2014, [Электронный ресурс], режим доступа: http://izvestia.ru/news/580240.
7. Бутузов С.Ю., Гвоздев Е.В. О первоочередных мероприятиях по обеспечению пожарной безопасности предприятия "мосводоканал", Интернет-журнал "Технологии техносферной безопасности" (http://ipb.mos.ru/ttb) Выпуск № 1 (59), 2015 г.
8. Вентцель Е.С. Теория вероятностей: Учеб. для вузов. — 6-е изд. стер. — М.: Высш. шк., 1999.— 576 с.
9. Волошин Г.Я., Бурлаков И.А., Косенкова С.Т., Статистические методы решения задач распознавания, основанные на аппроксимационном подходе, Владивосток, ТОИ ДВО РАН, 1992.
10. Волошин Г.Я., Методы распознавания образов, конспект лекций, Владивостокский государственный университет экономики и сервиса, г.

Владивосток, www.vvsu.ru, 2000.

11. Ворона В. А., Тихонов В. А., Системы контроля и управления доступом, М., Горячая линия-Телеком, 2010.
12. Выступление в Совете Федерации главы московского метрополитена Дмитрия Пегова, [Электронный ресурс], режим доступа: http://delate.info/41732-dmitriy-pegov-ezhednevno-metro-moskvy-perevozit-8-mln-chelovek.html.
13. Гнеденко Б. В. Курс теории вероятности. — 8-е изд. доп. и испр. — М.: Едиториал УРСС, 2005, ISBN 5-354-01091-8.
14. Гордиенко Д.М., Карпов А.В., Кириллов Д.С., Косачев А.А., Левченко Е.В., Шебеко Ю.Н. Данные о частотах возникновения пожаров и пожароопасных ситуаций в общественных зданиях различного назначения и на производственных объектах. Пожарная безопасность. 2009. № 2
15. Горелик А.Л., Скрипкин В.А., Методы распознавания, М., Высшая шк., 1977.
16. ГОСТ 27990-88, Средства охранной, пожарной и охранно-пожарной сигнализации. Общие технические требования, М., Издательство стандартов, 1988.
17. ГОСТ 50776-95, Системы тревожной сигнализации. Часть 1, раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию, М., Госстандарт России, 1995.
18. ГОСТ Р 22.0.02-94, Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий, М., Госстандарт России, 1995.
19. ГОСТ Р 50659-94, Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 2. Требования к извещателям. Общие положения, М., Госстандарт России, 1994.
20. ГОСТ Р 50775-95 (МЭК 60839-1-1:1988), Системы тревожной сигнализации. Часть 1. Общие требования, М., Госстандарт России, 1995.
21. ГОСТ Р 50776-95. Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию.
22. ГОСТ Р 52551-2006, Системы охраны и безопасности. Термины и определения, М., Стандартинформ, 2006.
23. Гусак А., Анализ существующих подходов к распознаванию лиц,

[Электронный ресурс], режим доступа: http://pcnews.ru/blogs/analiz_susestvuusih_podhodov_k_raspoznavaniu_lic-568865.html, 25.09.2014.

24. Дуда Р., Харт П., Распознавание образов и анализ сцен, М., Мир, 1976.
25. Ермолаев А., выступление на IT-форуме C-News 2012, Материалы C-News, [Электронный ресурс], режим доступа: www.cnews.ru, М., 2012.
26. Загоруйко Н.Г., Ёлкина В.Н., Емельянов С.В., Лбов Г.С., Пакет прикладных программ ОТЭКС, М., Финансы и статистика, 1986.
27. Загоруйко Н.Г., Методы распознавания и их применение, М., Советское радио, 1972.
28. Кельберт М. Я., Сухов Ю. М. Вероятность и статистика в примерах и задачах. Т. II: Марковские цепи как отправная точка теории случайных процессов и их приложения. М.: МЦНМО, 2009.
29. Китаев-Смык Л.А. Психология стресса: психологическая антропология стресса. М.: Академический Проект, 2009.
30. Конохов, Четыре миллиарда рублей на систему интеллектуального видеонаблюдения для Московского метрополитена, [Электронный ресурс], режим доступа: http://synesis.ru/industry/ transportnaya-infrastuktura.
31. Королюк В.С., Портенко Н.И.,Скороход А.В., Турбин А.Ф. Справочник по теории вероятностей и математической статистике. — М.: Наука, 1985.
32. Кузнецов А. О., Мусалимов В. М., Саенко А. П., Трамбицкий К. В. Применение алгоритмов анализа изображений для обнаружения пожаров: Изв. вузов. приборостроение. 2012. Т. 55, № 6.
33. Куликов А.А., Развитие и применение методов, алгоритмов и программных средств автоматической видео идентификации для предоставления индивидуального доступа по изображению лица, диссертация на соискание ученой степени кандидата технических наук, ФГБОУ ВПО «МАМИ», М., 2014.
34. Ладанов И.Д.. Психология управления рыночными структурами.- М., 1997.
35. Мазуров В.Д., Математические методы распознавания образов, уч. пособ. 2-е изд., доп. и перераб., Екатеринбург, изд. Уральского университета, 2010.
36. Марютина Т.М. Психофизиология эмоционально-потребностной сферы.

[Электронный ресурс], режим доступа: http://www.ido.edu.ru/psychology/psychophysiology/.

37. МДС 32-1.2000, Рекомендации по проектированию вокзалов, М., 1997, [Электронный ресурс], режим доступа: http://www.ohranatruda.ru/ot_biblio/normativ/data_normativ/5/5259/.
38. Местецкий Л. М., Математические методы распознавания образов, Курс лекций, МГУ, ВМиК, кафедра «Математические методы прогнозирования», 2002–2004.
39. Методика определения угроз безопасности информации в информационных системах. ФСТЭК России 2015 г.
40. Минаев В.А., Скрыль С.В., Овчинский А.С., Тростянский С.Н. Управление массовым сознанием: современные модели. М.: изд-во РосНОУ, 2013. 200 с.
41. Мирошник И.В. Теория автоматического управления. Линейные системы: Учебное пособие для вузов. - СПб.: Питер, 2005. - 336 с.
42. Морозов С.Н. Разработка и применение многопараметрических моделей управления персоналом с учетом типосенсорных индивидуальных особенностей. Диссертация на соискание ученой степени кандидата технических наук – М., 2002.
43. На систему интеллектуального видеонаблюдения для Московского метрополитена выделено 4 миллиарда рублей, [Электронный ресурс], режим доступа: http://habrahabr.ru/company/synesis/blog/212119.
44. Научно-образовательный курс «Поиск похожих фотографий в базе данных», http://mm-dsp.com/index.php?option=com_content&view=article&id=88:-q-q&catid=51:2013-07-11-10-58-26&Itemid=88.
45. Немчин Т.А. Состояния нервно-психического напряжения. Л., Изд-во ЛГУ, 1983.
46. Новиков Д.А., Петраков С.Н. Курс теории активных систем. М.: СИНТЕГ, 1999.
47. НПБ 110-03, Перечень зданий, сооружений, помещений и оборудования, подлежащих защите автоматическими установками тушения и обнаружения пожара, “Гарант”.
48. О.Креггер, Дж.М.Тьюсоон. Типы людей и бизнес.- М., 1995.

49. Описание характеристик системы «Каскад-поток», [Электронный ресурс], режим доступа: www.technoserv.com.
50. Патрик Э. Основы теории распознавания образов, М., Советское радио, 1980.
51. Петрова О., Райлян А., Обзор существующих методов биометрической идентификации. [Электронный ресурс], режим доступа: http://sec4all.net/modules/myarticles/ article.php?storyid=1265.
52. Пожары и пожарная безопасность в 2015 году: Статистический сборник. Под общей редакцией А.В. Матюшина. - М.: ВНИИПО, 2016.
53. Постановление Правительства Российской Федерации от 16.12.2013 №_1156 «Об утверждении Правил поведения зрителей при проведении официальных спортивных соревнований», Собрание законодательства Российской Федерации, 2013, № 51, ст. 6866.
54. Постановление Правительства Российской Федерации от 25.03.2015 № 272 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)», [Электронный ресурс], “Гарант”.
55. Постановление Правительства Российской Федерации от 25.12.2013 № 1244 «Об антитеррористической защищенности объектов (территорий)», [Электронный ресурс], “Гарант”.
56. Постановление Правительства РФ от 25.03.2015 г. № 272 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)»
57. Правила обеспечения безопасности при проведении официальных спортивных соревнований, утвержденные постановлением Правительства Российской Федерации от 18 апреля 2014 г. № 353, Собрание законодательства Российской Федерации, 2014, № 18, ст. 2194.
58. Пранов Б.М. Методы многомерных статистических исследований в проблемах техносферной безопасности, Интернет-журнал "Технологии техносферной безопасности" (http://ipb.mos.ru/ttb) Выпуск № 6 (52), 2013 г.

59. Приказ МВД России от 16.11.2006 № 937 «Об утверждении Инструкции по организации технической эксплуатации технических средств охраны на объектах, охраняемых подразделениями милиции вневедомственной охраны при органах внутренних дел Российской Федерации», М., 2006.
60. Приказ МВД России от 17.11.2015 г. № 1092 "Об утверждении Требований к отдельным объектам инфраструктуры мест проведения официальных спортивных соревнований и техническому оснащению стадионов для обеспечения общественного порядка и общественной безопасности"
61. Приказ МВД России от 18.01.2011 № 24 «О дополнительных мерах по обеспечению безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств», М., 2011.
62. Программа детектирования лиц, [Электронный ресурс], режим доступа: http://www.zeinet.kz/?docid=21.
63. Проклятие размерности [Электронный ресурс], режим доступа: http://www.machinelearning.ru/wiki/index.php?title=%D0%9F%D1%80%D0%BE%D0%BA%D0%BB%D1%8F%D1%82%D0%B8%D0%B5_%D1%80%D0%B0%D0%B7%D0%BC%D0%B5%D1%80%D0%BD%D0%BE%D1%81%D1%82%D0%B8
64. Прокуратура объявила об опознании всех жертв теракта в Ницце [Электронный ресурс], режим доступа: https://lenta.ru/news/2016/07/19/nicevictims/
65. Р 78.36.002-99, «Выбор и применение телевизионных систем видеоконтроля. Рекомендации», “Гарант”.
66. Р 78.36.005-99, «Выбор и применение систем контроля и управления доступом. Рекомендации», “Гарант”.
67. Р 78.36.007-99, «Выбор и применение средств охранно-пожарной сигнализации и средств технической укрепленности для оборудования объектов. Рекомендации», “Гарант”.
68. Распоряжение Правительства Российской Федерации от 27.08.2005 № 1314-р «Об одобрении Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов РФ», [Электронный ресурс],

“Гарант”.

69. Распоряжение Правительства РФ от 11 января 2011 г. №13-р «О бюджетных ассигнованиях на мероприятия по реализации проектов, одобренных Комиссией при Президенте Российской Федерации по модернизации и технологическому развитию экономики России», [Электронный ресурс], “Гарант”.
70. Распоряжение Правительства РФ от 3.12.2014 г. № 2446-р «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город».
71. Рекомендации по зонированию территории, антитеррористической защищенности и безопасности стадионов, принимающих матчи чемпионата мира по футболу FIFA 2018 года и Кубка конфедераций FIFA 2017 года, М., МВД, 2014.
72. Россия в цифрах. 2015: Крат.стат.сб./Росстат- М.,Р76 2015 - 543 с.
73. Россия в цифрах. 2016: Крат.стат.сб./Росстат- М.,Р76 2016 - 543 с.
74. Россия` 2012: Стат. справочник/ Р76 Росстат. – М., 2012. – 59 с.
75. Россия` 2013: Стат. справочник/ Р76 Росстат. – М., 2013. – 62 с.
76. Самаль Д.И., Алгоритмы идентификации человека по фотопортрету на основе геометрических преобразований, Институт технической национальной академии наук Беларуси, диссертация на соискание учёной степени кандидата технических наук, Минск, 2002.
77. Свод правил СП 132.13330.2011, «Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования», “Гарант”.
78. Системы биометрии, [Электронный ресурс], режим доступа: http://www.masterchop.rяu/articles/biometry/.
79. Сорокин Л.А. Автоматизированная система скрытой идентификации личности человека // Материалы 22-й международной научно-технической конференции "Системы безопасности – 2013". М.: Академия ГПС МЧС России, 2013. С. 246-249. http://ipb.mos.ru/sb/2013.
80. Сорокин Л.А. Кластерная информационная модель видеофиксации человеческой личности // Материалы 24-й международной научно-

технической конференции "Системы безопасности – 2015". М.: Академия ГПС МЧС России, 2015. http://ipb.mos.ru/sb/2015.

81. Сорокин Л.А. Распределенная модель хранения и поиска информации о личности на открытом множестве // Материалы IV Всерос.науч.-практ. конф. с междунар. уч. «Проблемы обеспечения безопасности при ликвидации последствий чрезвычайных ситуаций» Воронеж, ФГБОУ ВО Воронежский институт ГПС МЧС России., 2015., №1 с 436-439.
82. Состояние преступности в России за январь – май 2016 года [Электронный ресурс], режим доступа: https://xn--b1aew.xn--p1ai/upload/site1/document_news/007/968/943/sb_1605.pdf
83. СП 5.13130.2009. Установки пожаротушения и сигнализации. Нормы и правила проектирования, “Гарант”.
84. Средства контроля доступа// Иностранная печать о техническом оснащении полиции капиталистических государств . М.: ВИНИТИ. - 1992. -№ 4. - С.12-27.
85. Таранцев А. А. Применение регрессионного анализа для построения анизотропных и гистерезисных моделей, Автомат. и телемех., 1998, выпуск 5, 185–188.
86. Теракт в Ницце: новый метод и неотслеживаемый человек [Электронный ресурс], режим доступа: http://www.vesti.ru/doc.html?id=2776951
87. Тимошенко Д. М., Методы автоматической идентификации личности по изображениям лиц, полученным в неконтролируемых условиях, диссертация на соискание ученой степени кандидата технических наук, Санкт-Петербургский государственный университет, СПб., 2014.
88. Топольский Н.Г., Тетерин И.М., Чухно В.И., Рыженко А.А. Когнитивный центр управления системой комплексной безопасности пространственно-распределенных объектов с массовым пребыванием людей, Интернет-журнал "Технологии техносферной безопасности" (http://ipb.mos.ru/ttb) Выпуск № 6 (58), 2014 г.
89. Тропченко А.Ю., Методы вторичной обработки изображений и распознавания объектов, учебное пособие, СПб, СПбГУ ИТМО, 2012.
90. Указ Президента Российской Федерации от 15.02.2006 № 116 «О мерах по противодействию терроризму», “Гарант”.

91. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности», “Гарант”.
92. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности», “Гарант”.
93. Федеральный закон от 6.03.2006 № 35-ФЗ «О противодействии терроризму», “Гарант”.
94. Федоров А.В., Членов А.Н., Лукьянченко А.А., Буцынская Т.А., Демехин Ф.В.. Системы и технические средства раннего обнаружения пожара: Монография.— М.: Академия ГПС МЧС России, 2009
95. Фу К.С., Последовательные методы в распознавании образов и обучении машин, М., Наука, 1971.
96. Фу К.С., Структурные методы в распознавании образов, М., Мир, 1977.
97. Хрулев А., Системы распознавания лиц. Состояние рынка. Перспективы развития, Системы безопасности, № 1, 2012 г.
98. Членов А.Н., Климов А.В. Методика оценки эффективности системы безопасности объектов дистанционного банковского обслуживания, Интернет-журнал "Технологии техносферной безопасности" (http://ipb.mos.ru/ttb) Выпуск № 2 (60), 2015 г.
99. Ahonen, T., Hadid, A., and Pietikainen, M. Face Recognition with Local Binary Patterns. Computer Vision - ECCV 2004 (2004), 469–481.
100. Bartlett, M. S., Movellan, J. R., & Sejnowski, T. J. (2002) Face recognition by independent component analysis. IEEE Trans. Neural Networks, 13(6): 1450-1464.
101. Belhumeur P. N., Hespanha J. P., Kriegman D. J. Eigenfaces vs Fisherfaces: Recognition Using Class Specific Linear Projection // IEEE Transactions onPatern Analysis and Machine Intelligence. - 1997. - vol. 19. - PP.711-720.
102. Brunelli R., Poggio T. Face recognition: features versus templates // IEEE Transactions on Pattern Analysis and Machine Intelligence. - 1993. - vol.15. -№10.- PP. 1042-1052.
103. Dong Chen, Xudong Cao, Liwei Wang, Fang Wen, and Jian Sun. 2012.Bayesian face revisited: A joint formulation. In Proceedings of the 12th European Conference on Computer Vision
104. Ekman P. Strong evidence for universals in facial expressions // Psychol. Bull., 115(2): 268–287, 1994.

105. FaceVACS-DBScan // Cognitec Systems: [Электронный ресурс], режим доступа: http://www.cognitec.com/

106. Feng, Q., Pan, J. S., & Yan, L. (2012) Restricted nearest feature line with ellipse for face recognition. Journal of Information Hiding and Multimedia Signal Processing, 3(3): 297-305.

107. First Look at America's Supergun [Электронный ресурс], режим доступа: http://www.wsj.com/articles/a-first-look-at-americas-supergun-1464359194

108. Global Terrorism Index Report 2015, Institute for Economics and Peace, [Электронный ресурс], режим доступа: www.economicsandpeace.org.

109. Hyunjong Cho, Rodney Roberts, Bowon Jung, Okkyung Choi and Seungbin Moon, An Efficient Hybrid Face Recognition Algorithm Using PCA and GA-BOR Wavelets, Received 27 Jan, 2014; Accepted 12 Mar, 2014 DOI: 10.5772/58473.

110. ISO/IEC 11801:2002, Information technology - Generic cabling for customer premises.

111. Kamarainen, J. K., Kyrki, V., & Kalviainen, H. (2006) Invariance properties of Gabor filter-based featuresoverview and applications. IEEE Trans. Image Processing, 15(5): 1088-1099.

112. Kshirsagar, V. P., Baviskar, M. R., & Gaikwad, M. E. (2011) Face recognition using Eigenfaces. ICCRD 2011 3rd Int. Conf., 2: 302-306.

113. Lades, M., Vorbruggen, J. C., Buhmann, J., Lange, J., von der Malsburg, C., Wurtz, R. P., & Konen, W. (1993) Distortion invariant object recognition in the dynamic link architecture. IEEE Trans. Computers, 42(3): 300-311.

114. Lanitis, A., Taylor, C. J., & Cootes, T. F. (1995) Automatic face identification system using flexible appearance models. Image and Vision Computing, 13(5): 393-401.

115. Li, J. B., Chu, S. C., Pan, J. S., & Jain, L. C. (2012) Multiple Viewpoints Based Over-view for Face Recognition. Journal of Information Hiding and Multimedia Signal Processing, 3(4): 352-369.

116. Liu, C., & Wechsler, H. (2002) Gabor Feature Based Classification Using the Enhanced Fisher Linear Discriminant Model for Face Recognition. IEEE Trans. Image Processing, 11(4): 467-476.

117. Margot O'Neill, Amy Sherden Facial recognition: Privacy advocates raise

concern over 'creepy' system Government says will enhance national security [Электронный ресурс], режим доступа: http://www.abc.net.au/news/2015-09-09/national-facial-recognition-system/6761266.

118. Melinda Ham Face Recognition Technology [Электронный ресурс], режим доступа: http://www.uts.edu.au/about/faculty-law/news/face-recognition-technology.

119. Meng, J., & Yang, Y. (2012) Symmetrical twodimensional PCA with image measures in face recognition. Int. J. Adv. Robotic Sys., 9: 238-248.

120. Min, R., Hadid, A., & Dugelay, J. L. (2014) Efficient detection of occlusion prior to robust face recognition.The Scientific World Journal, Article ID 519158, pp.1-10.

121. Müller M., Röder T. Motion templates for automatic classification and retrieval of motion capture data. Symposium on Computer Animation — SCA. Viena, Austria, 2006, pp. 137–146.

122. Navon, D. (1977) Forest before trees: The precedence of global features in visual perception. Cognitive Psychology, 9(3): 353-383.

123. Oliva, A., & Torralba, A. (2006) Building the gist of a scene: The role of global image features in recognition. Progress in Brain Research, 155: 23-36.

124. Pentland, A., Moghaddam, B., & Starner, T. (1994) View-based and modular Eigen spaces for face recognition. IEEE CVPR on Computer Society Conference, p.84-91.

125. Rogers W. ETrue partners with Bio4 to combine facial biometrics//Biometric Digest. - 2001. - May. - P.4-5

126. Romdhani S. Face recognition using principal components analysis//MSc thesis.- University of Glasgow.- 1997.- P.183.

127. Rowley, H. A., Baluja, S., & Kanade, T. (1998) Neural network-based face detection. IEEE Trans. Pattern Analysis and Machine Intelligence, 20(1): 23-38.

128. Schneiderman, H., & Kanade, T. (1998, June). Probabilistic modeling of local appearance and spatial relationships for object recognition. IEEE CVPR on Computer Society Conference, 45-51.

129. Turk, M., & Pentland, A. (1991) Eigenfaces for recognition. Journal of Cognitive Neuroscience, 3(1): 71-86.

130. UK Government Standards Catalogue [Электронный ресурс], режим доступа: http://xml.coverpages.org/govtalkCat1.pdf

131. Valentin D., Abdi H., O'Toole. Categorization and identification of human, [Электронный ресурс], режим доступа: http://www.face-rec.org/interesting-papers/Other/abdi.vaeo97.pdf.

132. VeriLook SDK // Neurotechnology [Электронный ресурс], режим доступа: http://www.neurotechnology.com/

133. Wang Z., Yang X., Xu Y., Yu S. CamShift guided particle filter for visual tracking. Pattern Recognition Letters — PRL, 2009, vol. 30, no. 4, pp. 407–413.

134. Wiskott, L., Fellous, J. M., Kuiger, N., & Von Der Malsburg, C. (1997) Face recognition by elastic bunch graph matching. IEEE Trans. Pattern Analysis and Machine Intelligence, 19(7): 775-779.

135. Xu, Y., Li, Z., Pan, J. S., & Yang, J. Y. (2013) Face recognition based on fusion of multi-resolution Gabor features. Neural Computing and Applications, 23(5): 1251-1256.

136. Zhang, W., Shan, S., Gao, W., Chen, X., & Zhang, H. (2005) Local Gabor binary pat-tern histogram sequence (LGBPHS): A novel non-statistical model for face representation and recognition. ICCV, 1: 786-791.

137. Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003) Face recognition: A literature survey. ACM Computing Surveys (CSUR), 35(4): 399-458.

ПРИЛОЖЕНИЕ 1. СТРУКТУРА БД ИАС

Таблица 1 – Перечень полей ЦБД с указанием реквизитов

Название таблицы	Содержимое таблицы	Название столбца	Тип столбца	Описание столбца
People[2]	идентификационная информация о человеке, а также ссылки на таблицу с документами, удостоверяющими личность	id	Int	идентификатор интересанта, а также первичный ключ
		Name	varchar(35)	фамилия интересанта
		Surname	varchar(35)	имя
		Patronymic	varchar(35)	отчество
		BirthDay	Date	дата рождения
IdentDocument	информация о документах удостоверяющих личность	id	Int	идентификатор документа, а также первичный ключ
		idPeople	Int	внешний ключ для связи с таблицей People
		NameDoc	varchar(35)	название документа, например паспорт
		NumberDoc	Int	номер документа
		NamePeople	varchar(35)	фамилия интересанта
		SurnamePeople	varchar(35)	имя
		PatronymicPeople	varchar(35)	отчество
		Sex	varchar(1)	пол
		DirectoryPicture	varchar(256)	путь в файловой системе к расположению фотопортрета
Param-Doc	данные для связки таблицы IdentDocument с таблицей ParamDoc	idIdentDocument	Int	внешний ключ для связи с таблицей IdentDocument
		idParamDoc	Int	внешний ключ для связи с таблицей ParamDoc
ParamDoc	параметры документа, удостоверяющего личность, например, место рождения	id	Int	идентификатор параметра, а также первичный ключ
		Name	varchar(45)	имя параметра
		Value	varchar(45)	значение параметра
Log	история запросов оператора информации об интересанте	id	Int	идентификатор запроса, а также первичный ключ
		idSecurityOfficer	Int	идентификатор оператора, осуществившего запрос
		idPeople	Int	идентификатор интересанта, о котором запрошена информация

[2] Отметим, что учтено требование стандарта UK Government Standards Catalogue, согласно которому под имена и фамилии отводиться 35 символов [130].

		DateTime	datetime	дата и время запроса
Param-Log	данные для связки таблицы Log с таблицей ParamLog	idLog	Int	внешний ключ для связи с таблицей Log
		idParamLog	Int	внешний ключ для связи с таблицей ParamLog
ParamLog	параметры запроса оператора	Id	Int	идентификатор параметра, а также первичный ключ
		Name	varchar(45)	имя параметра
		Value	varchar(45)	значение параметра
SecurityOfficer	информация об операторах системы	Id	Int	идентификатор оператора, а также первичный ключ
		Name	varchar(35)	фамилия
		Surname	varchar(35)	имя
		Patronymic	varchar(35)	отчество
		BirthDay	Date	дата рождения
		IdentityDocument	varchar(35)	название документа, например паспорт
		NumberIdentity Document	Int	номер документа
Media	информация о директориях хранения файлов с изображением лица интересанта, полученных в ходе автоматического распознавания личности	Id	Int	идентификатор, а также первичный ключ
		idPeople	Int	внешний ключ для связи с таблицей People
		idHistory	Int	внешний ключ для связи с таблицей History
		idModel	Int	внешний ключ для связи с таблицей Model
		DirectoryPicture	varchar(256)	путь в файловой системе к расположению фотопортрета интересанта
Model	информация о математическом шаблоне лица, полученного в ходе автоматического распознавания на основе уникальности биометрии лица	id	Int	идентификатор шаблона, а также первичный ключ
		Name	varchar(45)	название метода, с использованием которого осуществлялось распознавание, например метод локальных бинарных шаблонов
		Rows	Int	количество строк в матрице математического шаблона лица
		Cols	Int	количество столбцов в матрице математического шаблона лица
		dt	varchar(35)	тип матрицы математического шаблона лица

Mat	информация о матрице математического шаблона лица	id	Int	идентификатор значения элемента матрицы
		idModel	Int	внешний ключ для связи с таблицей Model
		Data	Float	значения элемента матрицы
Param-Model	информация для связки таблицы Model с таблицей ParamModel	idParamModel	Int	внешний ключ для связи с таблицей ParamModel
		idModel	Int	внешний ключ для связи с таблицей Model
ParamModel	параметры математического шаблона лица	id	Int	идентификатор параметра, а также первичный ключ
		Name	varchar(45)	имя параметра
		Value	varchar(45)	значение параметра
History	информация о ЛБД, в которой хранится более детальная информация о местоположении физических лиц и их фотографий с камер видеонаблюдения	id	Int	идентификатор, а также первичный ключ
		DateTime	Datetime	дата и время видеофиксации
		idLStorage	Int	идентификатор локального хранилища объекта, на территории которого зафиксирован интересант
		idPeople	Int	идентификатор интересанта
LStorage	информация о локальном хранилище места массового скопления	id	int	идентификатор ЛБД
		ip	int	IP-адрес ЛБД
		Adress	varchar(256)	географический адрес места массового скопления людей
Param-LStorage	информация для связки таблицы LStorage с таблицей ParamLStorage	idLStorage	int	внешний ключ для связи с таблицей LStorage
		idParamLStorage	int	внешний ключ для связи с таблицей ParamLStorage
ParamLStorage	параметры ЛБД	Id	int	идентификатор параметра, а также первичный ключ
		Name	varchar(45)	имя параметра
		Value	varchar(45)	значение параметра

Таблица 2 – Перечень полей ЛБД с указанием реквизитов

Название таблицы	**Содержимое таблицы**	**Название столбца**	**Тип столбца**	**Описание столбца**
People	идентификационная информация о человеке, а также ссылки на таблицу с документами, удостоверяющими личность	id	int	идентификатор интересанта, а также первичный ключ
		Name	varchar(35)	фамилия
		Surname	varchar(35)	имя
		Patronymic	varchar(35)	отчество
		BirthDay	date	дата рождения
IdentDocument	информация о документах, удостоверяющих личность	id	int	идентификатор документа, а также первичный ключ
		idPeople	int	внешний ключ для связи с таблицей People
		NameDoc	varchar(35)	название документа, например паспорт
		NumberDoc	int	номер документа
		NamePeople	varchar(35)	фамилия
		SurnamePeople	varchar(35)	имя
		PatronymicPeople	varchar(35)	отчество
		Sex	varchar(1)	Пол
		DirectoryPicture	varchar(256)	путь в файловой системе к расположению фотопортрета интересанта
Param-Doc	данные для связки таблицы IdentDocument с таблицей ParamDoc	idIdentDocument	int	внешний ключ для связи с таблицей IdentDocument
		idParamDoc	int	внешний ключ для связи с таблицей ParamDoc
ParamDoc	параметры документа, удостоверяющего личность, например место рождения	id	int	идентификатор параметра, а также первичный ключ
		Name	varchar(45)	имя параметра
		Value	varchar(45)	значение параметра
Log	история запросов оператора информации об интересанте	id	int	идентификатор запроса, а также первичный ключ
		idSecurityOfficer	int	идентификатор оператора, осуществившего запрос
		idPeople	int	идентификатор интересанта, о котором запрошена информация
		DateTime	datetime	дата и время запроса
Param-Log	данные для связки таблицы Log с таблицей ParamLog	idLog	int	внешний ключ для связи с таблицей Log
		idParamLog	int	внешний ключ для связи с таблицей ParamLog

ParamLog	параметры запроса оператора	id	int	идентификатор параметра, а также первичный ключ
		Name	varchar(45)	имя параметра
		Value	varchar(45)	значение параметра
SecurityOfficer	информация об операторах системы	id	int	идентификатор оператора, а также первичный ключ
		Name	varchar(35)	фамилия
		Surname	varchar(35)	имя
		Patronymic	varchar(35)	отчество
		BirthDay	date	дата рождения
		IdentityDocument	varchar(35)	название документа, например паспорт
		NumberIdentity Document	int	номер документа
Media	информация о директориях хранения файлов с изображением лица интересанта, полученных в ходе автоматического распознавания личности	id	int	идентификатор, а также первичный ключ
		idPeople	int	внешний ключ для связи с таблицей People
		idHistory	int	внешний ключ для связи с таблицей History
		idModel	int	внешний ключ для связи с таблицей Model
		DirectoryPicture	varchar(256)	путь в файловой системе к расположению фотопортрета интересанта
Model	информация о математическом шаблоне лица, полученного в ходе автоматического распознавания на основе уникальности биометрии лица	id	int	идентификатор шаблона, а также первичный ключ
		Name	varchar(45)	название метода, с использованием, которого осуществлялось распознавание, например метод локальных бинарных шаблонов
		Rows	int	количество строк в матрице математического шаблона лица
		Cols	int	количество столбцов в матрице математического шаблона лица
		dt	varchar(35)	тип матрицы математического шаблона лица
Mat	информация о матрице математического шаблона лица	id	int	идентификатор значения элемента матрицы
		idModel	int	внешний ключ для связи с таблицей Model
		Data	float	значения элемента матрицы
Param-Model	информация для связки таблицы Model с таблицей ParamModel	idParamModel	int	внешний ключ для связи с таблицей ParamModel
		idModel	int	внешний ключ для связи с таблицей Model

ParamModel	параметры математического шаблона лица	id	int	идентификатор параметра, а также первичный ключ
		Name	varchar(45)	имя параметра
		Value	varchar(45)	значение параметра
History	информация о человеке: время фиксации, ссылка на информацию об адресе фиксации, ссылка на информацию о физическом лице и его психофизиологических показателях	id	int	идентификатор, а также первичный ключ
		DateTime	datetime	дата и время
		idCamera	int	идентификатор камеры, зафиксировавшей интересанта
		idPeople	int	идентификатор интересанта
		idCond	int	идентификатор психофизиологического состояния интересанта
		idPolygraph	int	идентификатор результатов проверки с использованием полиграфа
Camera	информация о камерах и их местоположении	id	int	идентификатор камеры, а также первичный ключ
		Adress	varchar(256)	адрес установки камеры
Param-Camera	информация для связки таблицы Camera с таблицей ParamCamera	idCamera	int	внешний ключ для связи с таблицей Camera
		idParamCamera	int	внешний ключ для связи с таблицей ParamCamera
ParamCamera	параметры камеры, например ее разрешительная способность	id	int	идентификатор параметра, а также первичный ключ
		Name	varchar(45)	имя параметра
		Value	varchar(45)	значение параметра
Condition[3]	информация о психофизиологическом портрете интересанта	id	int	идентификатор состояния, а также первичный ключ
		idBehavior	int	идентификатор поведения человека
		idEmotion	int	идентификатор эмоционального состояния человека

[3] В данной таблице перечислены показатели психофизиологического состояния интересанта, которые могут быть определены удаленно, без непосредственного привлечения интересанта. В частности, согласно работе [29] степень обилия потовыделений, уровень тремора, степень расширенности зрачков, температура – являются важнейшими показателями стресса, который испытывает интересант.

		idSweatRate	int	идентификатор, свидетельствующий о степени солевых выделениях
		idStrssLevel	int	идентификатор напряженности человека
		idTremorRate	int	идентификатор уровня тремора человека
		idExtensionPupils	int	идентификатор величины зрачков человека
		Temperature	decimal(5)	значение температуры человека
		SpecificDensity	int	значение удельной плотности человека; может использоваться для определения наличия посторонних тяжелых предметов под одеждой
		Other	varchar(45)	дополнительная информация о человеке, которая может быть заполнена оператором
Cndtn-Bhvr	информация для связки таблиц Condition и Behavior	idCondition	int	внешний ключ для связи с таблицей Condition
		idBehavior	int	внешний ключ для связи с таблицей Behavior
Behavior	информации о поведении интересанта	id	int	идентификатор поведения, а также первичный ключ
		Behavior	varchar(45)	описание поведения интересанта
Cndtn-Emtn	информация для связки таблицы Emotion с таблицей Condition и Polygraph	idCondition	int	внешний ключ для связи с таблицей Condition
		idPolygraph	int	внешний ключ для связи с таблицей Polygraph
		idEmotion	int	внешний ключ для связи с таблицей Emotion
Emotion[4]	информация об эмоциях интересанта	id	int	идентификатор эмоции, а также первичный ключ
		Emotion	varchar(45)	описание эмоции интересанта
TremorRate	информация об уровне тремора интересанта	id	int	идентификатор тремора, а также первичный ключ
		TremorRate	varchar(45)	уровень тремора интересанта
ExtensionPupils	информация о величине зрачков интересанта	id	int	идентификатор величины зрачков, а также первичный ключ
		Extension Pupils	varchar(45)	степень расширенности зрачков
SweatRate	информация об уровне солевых выделений интересанта	id	int	идентификатор, а также первичный ключ
		SweatRate	varchar(45)	степень солевых выделений

[4] В настоящее время распознавания эмоций зачастую основывается на мимических выражений лица. Определение эмоционального состояния можно осуществить на основе широко распространенной классификации, предложенной Полом Экманом [104]. Классификация представляет собой шесть эмоций, такие как счастье, печаль, гнев, страх, удивление и отвращение.

StrssLevel[5]	информация об уровне напряженности интересанта	id	int	идентификатор напряженности интересанта, а также первичный ключ
		StrssLevel	varchar(45)	уровень напряженности интересанта
KGR	информация о кожно-гальванической реакции человека	id	int	идентификатор реакции
		LP	decimal(5)	латентный период (секунды)
		A	decimal(5)	амплитуда (микровольты)
		T	decimal(5)	время первого колебания (секунды)
		Cnt	int	количество колебаний в первые три минуты
ExtTemperature	информация о температуре различных участков тела интересанта	id	int	идентификатор температурной реакции
		Forehead	decimal(5)	значение температуры лба
		Whiskey	decimal(5)	значение температуры висков
		Palm	decimal(5)	значение температуры ладоней
Polygraph[6]	информация о физиологических показателях состояния человека при его опросе с использованием детектора лжи	id	int	идентификатор вопроса и ответа человека, а также его состояния
		Question	varchar(1024)	содержимое вопроса
		Answer	varchar(1024)	содержимое ответа интересанта
		idSweatRate	int	идентификатор, свидетельствующий о степени солевых выделениях
		idExtensionPupils	int	идентификатор величины зрачков человека
		idTremorRate	int	идентификатор уровня тремора человека
		idStrssLevel	int	идентификатор напряженности человека
		idKGR	int	идентификатор кожно-гальванического рефлекса человека
		idEEG	int	идентификатор показателей, полученных с использованием метода электроэнцелографии

[5] Классификация уровней напряженности предоставляет дополнительные сведения о состоянии человека. Сейчас широко используется классификация, предложенная Т.А. Немчиным [45]: слабый, умеренный и чрезмерный уровень напряженности. Результаты, изложенные в статье [36], позволяют определять характеристики психологической напряженности так же, как и эмоционального состояния: по особенностям двигательных проявлений и, в частности, по мимическим выражениям лица. Для сравнения мимики лица с известными шаблонами и распознавания эмоций могут использоваться методы, применяемые для идентификации человека на основе уникальности биометрии.

[6] В данной таблице содержатся типичные физиологические показатели состояния человека при его опросе с использованием детектора лжи [45].

		idHeart	int	идентификатор состояния сердечно-сосудистой системы
		idExtTemperature	int	идентификатор температурных характеристик человека
		idBreath	int	идентификатор дыхания человека
EEG	информация о показателях датчиков электроэнцефалографии	id	int	идентификатор реакции
		Teta	int	значение ритма тета
		Alfa-1	int	значение ритма альфа-1
		Alfa-2	int	значение ритма альфа-2
		Beta-1	int	значение ритма бета-1
		Beta-2	int	значения ритма бета-2
Breath	информация о показателях пневмографа	id	int	идентификатор реакции
		AU	decimal(5)	значение амплитуды верхнего (грудного) дыхания
		FU	decimal(5)	значение частоты верхнего дыхания
		AD	decimal(5)	значение амплитуды нижнего (диафрагмального или брюшного) дыхания
		FD	decimal(5)	значение частоты нижнего дыхания
Heart	информация о сердечно сосудистой системе	id	int	идентификатор реакции
		Pulse	decimal(5)	пульс, удары в минуту
		Cycle	decimal(10)	значение сердечного цикла, секунды
		SystolicIndex	decimal(10)	систолический показатель
		PressureU	int	систолическое артериальное давление
		PressureD	int	диасистолическое артериальное давление

ПРИЛОЖЕНИЕ 2. МАКЕТЫ ДЕЙСТВИЙ РУКОВОДИТЕЛЯ И СОТРУДНИКОВ СЛУЖБЫ БЕЗОПАСНОСТИ

Таблица 1 – Описание действий руководителя объекта (группы объектов)

№	Наименование мероприятия	Ответственный
1	**Оценка обстановки на объекте:** - получение данных о выявленных ПОЛ; -получение данных о возможных местах появления ПОЛ; - постановка задач операторам о ведении наблюдения на объекте с учётом полученных данных; - проведение проверок полученных данных и постановка дополнительных аналитических задач операторам.	
2	**Организация работ:** - постановка задач о ведении наблюдения на объекте по поиску интересантов и выявлении ПОЛ и их возможных соучастников; - решение о постановке задач на наблюдение с определенных камер.	
3	**Организация взаимодействия:** - контроль доведение информации до обязательных подразделений, например МВД; - контроль передачи информации другим заинтересованным подразделениям.	
4	**Планирование мероприятий:** - организация и контроль процессов разработки планов по поиску и сопровождению интересантов; - планирование и постановка задач подчиненным подразделениям по вновь выявленным ПОЛ.	
5	**Анализ докладов и информации** от - операторов по поиску интересантов и выявлению ПОЛ, в частности получение статистических данных по их адресам появления и соучастникаv; - территориальных органов исполнительной власти и организаций, чьи силы и средства задействованы для поиска интересантов и мониторинга ПОЛ.	
6	**Подготовка докладов** о ходе работ по поиску интересантов и мониторингу интересантов.	
7	**Контроль деятельности подчиненных органов управления** и исполнения ими распоряжений в процессе поиска интересантов и мониторинга ПОЛ.	
8	**Представление информации** об обнаруженных ПОЛ и их соучастниках средствам массовой информации через отдел информации и связи с общественностью.	
9	**Координация действий** заинтересованных подразделений при поиске интересантов и мониторинге ПОЛ.	
10	**Учет принятых решений**, отданных распоряжений и полученных донесений в хронологической последовательности.	
11	**Участие в экспертных оценках** эффективности системы и работы операторов подразделения.	
12	**Обобщение опыта** работы по поиску интересантов и мониторингу ПОЛ, выработка предложений по совершенствованию системы реагирования на ПОЛ, подготовка отчетов о проделанной работе.	

Таблица 2. – Описание действий оператора

№	Наименование мероприятия	Ответственный
1	**Ведение наблюдения и оценка текущей обстановки на объекте:** - мониторинг ПОЛ на объекте; - ввод данных в систему и получение информации о возможных местах появления интересантов; - доведение предложений о ведении наблюдения на объекте с учётом полученных данных; - оценка эмоционального состояния и психологического напряжения интересантов по внешним признакам.	
2	**Поиск интересантов:** - получение данных о фотографиях и фотороботах интересантов; - постановка системе задач по поиску интересантов на основе биометрии лица; - постановка системе задач по поиску интересантов на основе информации о событиях; -проведение анализа статистических данных о возможных соучастниках интересантов; - проведение анализа статистических данных по адресам появления интересантов; - на основе данных об адресах и времени появления интересантов и их соучастников, получение дополнительной информации, в частности о предположительном месте работы, проживания, вероисповедании, вкусах, уровне культурного развития и прочее; - постановка задач на наблюдение с камер в районах наиболее частого их появления; - проведение проверок полученных данных и постановка системе дополнительных аналитических задач.	
3	**Доведение информации:** - доведение информации до руководства; - доведение информации до других операторов в части, касающейся поиска подозрительных лиц.	
4	**Осуществление взаимодействия:** - доведение информации до обязательных подразделений; - согласованная передача информации другим заинтересованным подразделениям.	
5	**Планирование мероприятий**: - разработка планов оперативного сопровождения ПОЛ на основе данных из системы; - планирование задач по вновь выявленным ПОЛ.	
6	**Обобщение докладов** из района от оперативной группы, а также территориальных органов исполнительной власти и организаций, чьи силы и средства задействованы для поиска интересантов и мониторинга ПОЛ.	
7	**Подготовка докладов** о ходе работ по поиску интересантов и мониторингу интересантов.	
8	**Представление информации** об обнаруженных ПОЛ и их соучастниках средствам массовой информации через отдел информации и связи с общественностью.	
9	**Выработка предложений по** поиску интересантов и мониторингу ПОЛ.	
10	**Участие в экспертных оценках** эффективности системы и работы операторов подразделения.	
11	**Обобщение опыта** работы по поиску интересантов и мониторингу ПОЛ, выработка предложений по совершенствованию системы реагирования на ПОЛ, подготовка отчетов о проделанной работе.	

ПРИЛОЖЕНИЕ 3. СВИДЕТЕЛЬСТВО О ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ПРОГРАММЫ ДЛЯ ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2016663708

«ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ МОДЕЛЬ ПОДДЕРЖКИ УПРАВЛЕНИЯ ИДЕНТИФИКАЦИЕЙ ЛИЧНОСТИ НА ОСНОВЕ ТЕОРИИ РАСПОЗНАВАНИЯ ОБРАЗОВ»

Правообладатели: *Сорокин Леонид Андреевич (RU), Бутузов Станислав Юрьевич (RU)*

Авторы: *Сорокин Леонид Андреевич (RU), Бутузов Станислав Юрьевич (RU)*

Заявка № **2016661867**
Дата поступления **27 октября 2016 г.**
Дата государственной регистрации в Реестре программ для ЭВМ ***14 декабря 2016 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

ПРИЛОЖЕНИЕ 4. АКТЫ ВНЕДРЕНИЯ

МВД России
Главное управление Министерства внутренних дел Российской Федерации по г. Москве
Управление внутренних дел по Центральному административному округу
ГУ МВД России по г. Москве
Отделение полиции по обслуживанию Олимпийского комплекса «Лужники»
Москва, Лужнецкий проезд, дом 24
Телефон (495) 245-37-64,
факс (499) 246-63-93
15.09.2017 № 1/27-201а
на № _____ от _____

УТВЕРЖДАЮ
Начальник отдела полиции по обслуживанию ОК «Лужники» УВД по ЦАО ГУ МВД России по городу Москве
полковник полиции
С.А. Шорин
«___» 2017 г.

АКТ
о внедрении результатов кандидатской диссертационной работы Сорокина Леонида Андреевича

Результаты диссертационной работы Сорокина Леонида Андреевича, в частности:

- алгоритмы формирования и управления комплексом мероприятий пожарной и криминальной безопасности;
- оценка эффективности управления безопасностью на основе многопараметрической модели;
- требования к персоналу службы безопасности с учетом профессиональных качеств, личностных факторов и особенностей сенсорной системы

рекомендованы к использованию для противодействия общественно-опасным преступным проявлениям и обеспечения общественного порядка при проведении массовых мероприятий на территории Олимпийского комплекса «Лужники».

Заместитель начальника ОП ООК «Лужники»
подполковник полиции — В.А. Рудык

Заместитель начальника ОП ООК «Лужники»
старший лейтенант полиции — Д.С. Болденков

Начальник ОУР ОП ООК «Лужники»
майор полиции — Р.И. Сергеев

Общество с ограниченной ответственностью
«Инженерно-Техническая Компания»
РФ, 109145, г. Москва, ул. Привольная, д.2, корп.5, помещение XI, эл. почта: expert_int@mail.ru, тел: 8-968-379-33-34, ИНН 9721030181, ОГРН 5167746423917

Исх № 42 от «19» марта 2017 г.

О внедрении

УТВЕРЖДАЮ
Директор ООО «Инженерно-Техническая Компания»
_____ В.А. Капрош
«19» марта 2017 г.

АКТ

об использовании результатов диссертационной работы
Сорокина Леонида Андреевича

Настоящим подтверждаем, что результаты диссертационной работы Сорокина Леонида Андреевича, а именно:

- математическая модель поддержки управления безопасностью, позволяющая стабилизировать функционирование объектов с массовым пребыванием людей;
- семейство алгоритмов формирования и поддержки управления безопасностью в объектах с массовым пребыванием;
- новый гибридный алгоритм распознавания лиц;
- новые структуры базы данных об интересанте,

обладают актуальностью, представляют интерес и рекомендуются к использованию при разработке автоматизированных систем поддержки управления безопасностью. Применение данных результатов способствуют повышению безопасности объектов общественного назначения и мест массового пребывания людей.

Председатель комиссии:
Заместитель директора _____ О.С. Трунтаева

Члены комиссии:
Руководитель проектов _____ Е.Г. Сотникова

Главный технический специалист _____ А.В. Ветшко