Министерство науки и высшего образования Российской Федерации
Филиал федерального государственного автономного образовательного учреждения высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)» в г. Миассе
Факультет «Электротехнический»
Кафедра «Автоматика»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой
_____ С.С. Голощапов
_____ 2018 г.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА КОНТРОЛЯ ДОСТУПА НА ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ–270304.2018.850.00 ПЗ ВКР

Руководитель проекта
старший преподаватель
_____ О.В. Константинова
_____ 2018 г.

Автор проекта
студент группы МиЭт–598
_____ А.И. Павличенко
_____ 2018 г.

Нормоконтролер
доцент, к.т.н.
_____ Т.А. Барбасова
_____ 2018 г.

Миасс 2018

АННОТАЦИЯ

Павличенко А.И. Автоматизированная система контроля доступа на производственное предприятие Челябинское ЛПУ. – Миасс: Филиал «ФГАО ВО ЮУРГУ (НИУ)», Эт; 2018, 108 с., 40 ил., библиогр. список – 50 наим. 1 прилож., 2 листа алгоритмов ф А4, 1 лист схема ф А3.

Рассматривается проект модернизации внедряемой на предприятии АСКУД за счет добавления к ней функционала распознавания лиц на основе связанного с АСКУД программного модуля, использующего библиотеку компьютерного зрения с открытым исходным кодом OpenCV от INTEL.

					270304.2018.850.00 ПЗ			
Изм.	Лист	№ докум.	Подпись	Дата				
Разраб.		Павличенко А.И.			Автоматизированная система контроля доступа на производственное предприятие Челябинское ЛПУ	Лит	Лист	Листов
Пров.		Константинова О.В.				Д	5	108
						ЮУрГУ Кафедра Автоматики		
Н. контр.		Барбасова Т.А.						
Утв.		Голощапов С.С.						

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Одной из важнейших задач обеспечения безопасности жизнедеятельности человека является контроль и управление перемещением людей или предметов по определенным маршрутам и зонам. Как примеры можно привести контроль допуска служащих на предприятие; людей в подъезды дома, в котором они живут; обнаружение выноса неоплаченных товаров из магазина или проноса неразрешенных к провозу в самолете предметов и т. д. Все это может решаться системами контроля и управления доступом (СКУД) [1].

В общем случае под СКУД обычно понимают совокупность программно–технических и организационно–методических средств, с помощью которых решается задача контроля и управления замкнутыми территориями, зданиями целиком и отдельными помещениями внутри них. На промышленном предприятии, помимо вышеперечисленных, СКУД решает задачи оперативного контроля за передвижением персонала и времени его нахождения на территории предприятия.

Первичная функция любой СКУД на предприятии – пропускать тех, кому этот вход разрешен, и не пропускать тех, кому вход запрещен. Все ее остальные функции следуют из базовой и могут служить таким целям, как:

- противодействие промышленному шпионажу;
- противодействие воровству;
- противодействие терроризму;
- противодействие саботажу;
- противодействие умышленному повреждению материальных ценностей;
- учет рабочего времени;
- контроль своевременности прихода и ухода сотрудников;
- защита конфиденциальности информации;
- регулирование потока посетителей;
- контроль въезда и выезда транспорта.

Кроме этого, СКУД является барьером для «любопытных» [2].

Направление деятельности предприятия, его масштаб, структура, внутренняя организация его технологических и управленческих процессов, а также многое другое определяют особенности реализации СКУД и делают каждый такой проект уникальным для отдельного предприятия. Это могут быть как самые простейшие системы с одной точкой доступа в помещение, так и распределенные сетевые программно–аппаратные комплексы, охватывающие обширную территорию завода и имеющие в своем составе десятки и сотни точек доступа и даже включенные в единую систему учета производственной деятельности предприятия.

На сегодняшний день уровень развития технологий позволяет реализовывать СКУД, роль человека в которых стремительно снижается, что позволяет говорить о таких системах, как об автоматизированных системах контроля и управления доступом (АСКУД). Все более доступными и популярными становятся технологии бесконтактной и биометрической идентификации: по отпечаткам пальцев, сетчатке глаза, по лицу. Использование подобных решений оправданно, поскольку уменьшается вероятность человеческой ошибки в процессе идентификации и одновременно повышается скорость принятия решения о допуске субъекта, что особенно актуально на средних и крупных предприятиях, где в начале и конце рабочего дня поток сотрудников, пропускаемых через проходные, может составлять до нескольких сотен человек за раз.

В выпускной квалификационной работе будет представлен проект модернизации внедряемой на предприятии АСКУД за счет добавления к ней функционала распознавания лиц на основе связанного с АСКУД программного модуля, использующего библиотеку компьютерного зрения с открытым исходным кодом OpenCV от INTEL.

1. СКУД на современном промышленном предприятии

1.1 Принципы проектирования СКУД на предприятии и предъявляемые при постановке задачи требования

Для понимания принципов проектирования и построения СКУД необходимо знать, что эта система является такой же частью мероприятий и процессов обеспечения безопасности на предприятии, как и прочие: экономическая безопасность, патрулирование объектов и территории, досмотры сотрудников и транспорта и т.п. А значит, при разработке техзадания на построение СКУД исходят из такого основополагающего для системы безопасности понятия как контрольно–пропускной режим (КПР).

КПР – комплекс организационно–правовых ограничений и правил, устанавливающих порядок пропуска через контрольно–пропускные пункты (КПП) в отдельные здания (помещения) людей, транспорта и материальных средств.

КПР реализуется посредством применения «запретов» и «ограничений» в отношении субъектов, пересекающих границы охраняемых объектов, для обеспечения интересов предприятия. Такой механизм должен соответствовать требованиям действующего законодательства, уставу предприятия, а также иным нормативно–правовым актам, регулирующим деятельность предприятия. Основные направления создания КПР на предприятии: определение и оценка исходных данных, разработка мероприятий и нормативных документов, оборудование КПП. Система контроля и управления доступом является третьим рубежом защиты после системы видеонаблюдения и охранно–пожарной сигнализации.

В числе решаемых КПР как частью системы безопасности задач:

– обеспечение санкционированного прохода сотрудников и посетителей, ввоза/вывоза продукции и материальных ценностей, ритмичной работы предприятия;

– предотвращение бесконтрольного проникновения посторонних лиц и транспортных средств на охраняемые территории и в отдельные здания

(помещения);

– своевременное выявление угроз интересам предприятия, а также потенциально опасных условий, способствующих нанесению предприятию материального и морального ущерба.

Основные мероприятия КПР разрабатываются службой безопасности предприятия, утверждаются его руководителем и оформляются инструкцией о КПР.

Ответственность за организацию КПР возлагается на начальника службы безопасности. Практическое осуществление КПР возлагается на охрану (дежурных по КПП, контролеров, охранников), работники которой должны знать установленные на объекте правила КПР, действующие документы по порядку пропуска на объект (с объекта) сотрудников и посетителей, ввоза/вывоза товарно–материальных ценностей.

КПР может быть установлен как в целом по предприятию, так и в отдельных корпусах, зданиях, отделах и других специальных помещениях [2].

Разработка мероприятий и нормативных документов КПР начинается с определения исходных данных, к которым относятся:

1. Организационная структура предприятия, расположение его отдельных элементов и характер производства (деятельности) на них. Выяснение этих вопросов позволяет решить следующие практические задачи:

– выделить объекты, площадки, здания и помещения, на которых необходимо организовать КПР;

– определить характер КПП для пропуска сотрудников и транспортных средств;

2. Оценка «суточного объема» потоков транспортных средств, грузов, материальных ценностей и людей (персонала фирмы и посетителей), проходящих через КПП и в отдельные здания (помещения). Только на основе оценки реального состояния мест пропуска можно оценить пропускную способность действующих КПП и привести ее в соответствие с задачами объекта. Такая оценка позволит выбрать оптимальный вариант автоматизации и контроля прохода (проезда) на охраняемые территории.

3. Выделение (по степени важности) категории объектов, транспортных средств

и грузов, а также категории лиц, пересекающих установленные границы. Для достижения четкости в определениях предлагается помещения и территорию объекта классифицировать в зависимости от условий доступа и степени защищенности.

Для организации пропускного режима также необходимо распределить объекты предприятия (здания, помещения) на следующие зоны: общедоступные, закрытые и ограниченного доступа. Определение категорий режима может дать четкий ответ на вопросы, которые нужно прояснить при организации КПР и разработке исходной документации по оборудованию объекта техническими средствами охраны. Закрепление за помещением конкретной категории помогает регламентировать и обосновать:

– условия доступа сотрудников предприятия и посетителей в ту или иную зону;

– предложения администрации предприятия по выработке оптимального варианта порядка пропуска лиц, транспортных средств и материальных ценностей на объекты предприятия;

– наличие и вид физической охраны;

– виды используемых технических средств для обеспечения безопасности.

В свою очередь, разработанный и утвержденный КПР является первоисточником требований к проектируемой СКУД, ее параметрам и характеристикам.

Помимо обозначенных на этапе разработки КПР вопросов, при проектировании СКУД, как правило, крайне важно учесть как можно больше нюансов в технической части, поскольку при эксплуатации системы любой забытый или неучтенный момент может существенно снизить эффективность ее работы или же и вовсе перечеркнуть большинство преимуществ ее использования.

К таким вопросам можно отнести:

1) Работа системы в аварийных режимах (сбой в работе, пожарная тревога и др.): резервирование электропитания на случай отключения основного, минимизация создания помех эвакуации сотрудников и техники, прежде всего заключающаяся в возможности быстрой разблокировки дверей, возможно, без участия системы, возможности автономной работы отдельных устройств

системы в случае повреждения линий связи между ними;

2) правильный выбор канала связи для распределенных систем: здесь нужно руководствоваться критериями надежности и отказоустойчивости, количеством и типом управляемых СКУД устройств, а также их удаленностью от контроллеров;

3) защищенность СКУД от несанкционированного воздействия: легкий доступ к замку, считывателю, контроллеру и блоку питания, устаревшие форматы и базирование на протоколах, не позволяющих применить надежные недорогие средства защиты информации, отсутствие стратегии на случай повреждения линий связи, контроллера, сервера, памяти и прочего оборудования СКУД, которое может привести к несанкционированным или неучтенным проходам, отсутствие сигнализации о взломах дверей – все это лишает смысла затраты на СКУД;

4) возможности масштабирования системы в будущем: ограничения управляющего оборудования по количеству управляемых устройств, пропускной способности каналов связи, подключение новых устройств, в том числе, других производителей [3].

1.2 Общие технические требования, предъявляемые к СКУД

В разделе 5 ГОСТ Р 51241–98 [4, п.5] определены технические требования к СКУД. Среди требований общего характера выделим такие:

– средства и системы контроля и управления доступом (КУД) должны обеспечивать возможность как круглосуточной, так и сменной работы, с учетом проведения регламентного технического обслуживания;

– средства КУД, предназначенные для построения систем, должны обладать конструктивной, информационной, надежностной и эксплуатационной совместимостью.

Теперь рассмотрим требованиям к функциональным характеристикам СКУД.

Автономные системы КУД должны обеспечивать:

– открывание устройств преграждающих управляемых (УПУ) при считывании зарегистрированного в памяти системы идентификационного признака;

– запрет открывания УПУ при считывании незарегистрированного в памяти системы идентификационного признака,

– запись идентификационных признаков в память системы;

– защиту от несанкционированного доступа при записи кодов идентификационных признаков в памяти системы;

– сохранение идентификационных признаков в памяти системы при отказе и отключении электропитания;

– ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;

– автоматическое формирование сигнала сброса на УПУ при отсутствии факта прохода;

– выдачу сигнала тревоги при использовании системы аварийного открывания УПУ для несанкционированного проникновения.

Дополнительные характеристики автономных систем в зависимости от класса

по функциональным характеристикам приведены в Таблица 1.

Таблица 1 – Функциональные характеристики автономных систем

Функциональные характеристики автономной системы	**Класс системы**		
	1	**2**	**3**
1. Установка уровней доступа	–	+/–	+
2. Установка временных интервалов доступа	–	+/–	+
3. Возможность установления времени открывания УПУ	–	+/–	+
4. Защита от повторного использования идентификатора для прохода в одном направлении	–	+/–	+
5. Ввод специального идентификационного признака для открывания под принуждением	–	+/–	+
6. Подключение УВИП различных типов	–	+/–	+/–
7. Световая индикация о состоянии доступа	+/–	+	+
8. Контроль состояния УПУ	+/–	+	+
9. Световое и (или) звуковое оповещение о попытках НСД	+/–	+/–	+
10. Регистрация и хранение информации о событиях в энергонезависимой памяти	–	+	+
11. Количество событий, хранимых в энергонезависимой памяти, не менее	–	16	64
12. Ведение даты и времени возникновения событий	–	+/–	+
13. Возможность подключения принтера для вывода информации	–	+/–	+
14. Возможность передачи информации на устройства сбора информации или ЭВМ	–	+/–	+
15. Возможность объединения в сеть и обмена информацией с устройствами сбора информации и управления (ЭВМ)	–	+/–	+
16. Возможность интегрирования с системой охранной и (или) пожарной сигнализации на релейном уровне	–	+/–	+
17. Возможность интегрирования с системой видеоконтроля на релейном уровне	–	+/–	+
18. Возможность подключения дополнительных средств специального контроля, средств досмотра	–	–	+/–
Примечание. Условный знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «–» – отсутствие функции, а знак «+/–» – наличие или отсутствие функции.			

Системы КУД с централизованным управлением и универсальные должны соответствовать вышеперечисленным требованиям и дополнительно обеспечивать:

1) регистрацию и протоколирование тревожных и текущих событий;
2) приоритетное отображение тревожных событий;
3) управление работой УПУ в точках доступа по командам оператора;
4) задание временных режимов действия идентификаторов в точках доступа «окна времени» и уровней доступа;
5) защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации;
6) автоматический контроль исправности средств, входящих в систему, и линий передачи информации;
7) возможность автономной работы контроллеров системы с сохранением контроллерами основных функций при отказе связи с пунктом централизованного управления;
8) установку режима свободного доступа с пункта управления при аварийных ситуациях и чрезвычайных происшествиях (пожар, землетрясение, взрыв и т.п.);
9) блокировку прохода по точкам доступа командой с пункта управления в случае нападения;
10) возможность подключения дополнительных средств специального контроля, средств досмотра.

Дополнительные характеристики систем с централизованным управлением, в зависимости от класса по функциональным характеристикам, приведены в Таблица 2.

Таблица 2 – Функциональные характеристики систем с централизованным управлением и универсальных

Функциональные характеристики систем с централизованным управлением (сетевых) и универсальных	Класс системы		
	1	**2**	**3**
1. Количество уровней доступа	2	8	16
2. Количество временных интервалов доступа	2	8	16
3. Защита от повторного использования идентификатора для прохода в одном направлении	+/–	+	+
4. Ввод специального идентификационного признака для открывания под принуждением	+/–	+	+
5. Подключение устройств ввода идентификационных признаков	+/–	+	+
6. Доступ по «правилу двух (и более) лиц»	+/–	+/–	+
7. Количество событии, сохраняемых в энергонезависимой памяти контроллеров, не менее	50	250	1000
8. Возможность интегрирования с системой охранной и (или) пожарной сигнализации на релейном уровне	+	+/–	+/–
9. Возможность интегрирования с системой видеоконтроля на релейном уровне	+	+/–	+/–
10. Возможность интегрирования с системой охраной, пожарной сигнализации и системами видеоконтроля на системном уровне	+/–	+/–	+
11. Возможность управления работой дополнительных устройств в точках доступа (освещение, вентиляция, лифты, технологическое оборудование и т. п.)	–	+/–	+/–
12. Возможность подключения переговорных устройств и (или) средств связи в точках доступа	–	+/–	+/–
13. Обеспечение изображения на экране ЭВМ плана объекта и (или) помещений объекта с указанием мест расположения средств контроля доступа, охранной и пожарной сигнализации, средств видеоконтроля и графическим отображением тревожных состояний в контрольных точках на плане	+/–	+/–	+
14. Интерактивное управление средствами по изображению плана объекта на экране ЭВМ	–	–	+/–
15. Ведение баз данных на сотрудников (пользователей)	+/–	+	+
16. Поддержание фотографических данных пользователей в базе данных	–	+/–	+
17. Контроль за перемещением и поиск сотрудников	+/–	+/–	+
18. Контроль времени нахождения на объекте посетителей	+/–	+/–	+
Примечание. Условный знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «–» – отсутствие функции, а знак «+/–» – наличие или отсутствие функции.			

Системы КУД должны также иметь следующие характеристики, значения которых должны быть установлены в стандартах и (или) технических условиях на системы конкретного типа:

– максимальное количество точек доступа, зон доступа, пользователей, обслуживаемых системой;

– максимальное количество точек доступа, обслуживаемых одним устройством управления (УУ);

– количество и вид временных интервалов доступа (окон времени), уровней доступа;

– количество видов УВИП, используемых в системе;

– время реакции системы на заявку на проход;

– максимальное расстояние от наиболее удаленной точки доступа до пункта управления;

– максимальное расстояние действия считывателя (для бесконтактных считывателей);

– максимальное время хранения информации о событиях в памяти системы;

– максимальная пропускная способность системы в точках доступа;

– вероятность несанкционированного доступа, вероятность ложного задержания (требования обязательны для СКУД с биометрической идентификацией, для остальных допускается не указывать);

– показатели по уровням устойчивости к НСД.

ГОСТ устанавливает требования к функциональным характеристикам и конкретно на такой ключевой компонент СКУД, как УПУ:

1) полное или частичное перекрытие проема прохода;

2) ручное, полуавтоматическое или автоматическое управление;

3) блокирование человека или объекта для УПУ блокирующего типа;

4) УПУ в дежурном режиме могут быть в нормально открытом или нормально закрытом состоянии;

5) УПУ с частичным перекрытием проема прохода могут быть, при необходимости, обеспечены средствами сигнализации, срабатывающими при

попытке обхода заграждающего устройства;

6) для УПУ, используемых на проходных или в других местах с большими потоками людей, в стандартах или технических условиях на УПУ конкретного типа должны быть установлены показатели пропускной способности;

7) УПУ в закрытом состоянии должны обеспечивать физическое препятствие перемещению людей, транспорта и других объектов в (из) помещение, здание, зону или на территорию и открывание запирающего механизма при подаче управляющего сигнала от устройства управления;

8) нормально закрытые УПУ могут быть оборудованы средствами звуковой сигнализации, которая включается после их открывания и при отсутствии прохода в течение установленного времени, или могут иметь средства для возврата в закрытое состояние;

9) УПУ при необходимости могут иметь защиту от прохода через них одновременно двух или более человек;

10) УПУ должны иметь возможность механического аварийного открывания в случае пропадания электропитания, возникновения пожара или других стихийных бедствий. Аварийная система открывания должна быть защищена от возможности использования ее для несанкционированного проникновения;

11) умышленное повреждение внешних электрических соединительных цепей и элементов блокировки не должно приводить к открыванию УПУ;

12) должны быть предусмотрены меры по защите внешних электрических соединительных цепей от возможности подачи по ним напряжений, приводящих к нарушению работы или к открыванию УПУ.

Требования к функциональным характеристикам УВИП:

1) возможность считывания идентификационного признака с идентификаторов;

2) введение биометрической информации (для считывателей биометрической информации);

3) преобразование введенной информации в электрический сигнал;

4) передачу информации на УУ;

5) УВИП должны быть защищены от манипулирования путем перебора и

подбора идентификационных признаков. Виды защиты должны быть указаны в стандартах и (или) нормативных документах на УВИП конкретного типа;

6) идентификаторы УВИП должны обеспечивать хранение идентификационного признака в течение срока службы и при эксплуатации;

7) конструкция, внешний вид и надписи на идентификаторе и считывателе не должны приводить к раскрытию применяемых кодов;

8) производитель идентификаторов должен гарантировать, что код данного идентификатора не повторится, или указать условия повторяемости кода и меры по предотвращению использования идентификаторов с одинаковыми кодами;

9) считыватели УВИП при взломе и вскрытии, а также в случае обрыва или короткого замыкания подходящих к ним цепей не должны вызывать открывание УПУ. При этом автономные системы могут выдавать звуковой сигнал тревоги, а системы с централизованным управлением сигнал тревоги могут передавать на пункт управления и, при необходимости, выдавать звуковой сигнал.

Требования к функциональным характеристикам УУ:

1) аппаратные средства УУ должны обеспечивать прием информации от УВИП, обработку информации и выработку сигналов управления на исполнительные устройства УПУ;

2) аппаратные средства УУ в системах с централизованным управлением и универсальных должны обеспечивать:

– обмен информацией по линии связи между контроллерами и средствами управления;

– сохранность данных в памяти при обрыве линий связи со средствами централизованного управления, отключении питания и при переходе на резервное питание;

– контроль линий связи между контроллерами, средствами централизованного управления. Протоколы обмена информацией должны обеспечивать необходимую помехоустойчивость, скорость обмена информацией, а также, при необходимости, защиту информации;

3) программное обеспечение УУ должно обеспечивать:

– занесение кодов идентификаторов в память системы;

– задание характеристик точек доступа;

– установку временных интервалов доступа (окон времени);

– установку уровней доступа для пользователей;

– протоколирование текущих событий;

– ведение и поддержание баз данных;

– регистрацию прохода через точки доступа в протоколе базы данных;

– сохранение баз данных и системных параметров на резервном носителе;

– сохранение баз данных и системных параметров при авариях и сбоях в системе;

– приоритетный вывод информации о нарушениях;

– возможность управления УПУ в случае чрезвычайных ситуаций;

4) программное обеспечение УУ должно быть устойчиво к случайным и преднамеренным воздействиям следующего вида:

– отключение питания аппаратных средств;

– программный сброс аппаратных средств;

– аппаратный сброс аппаратных средств;

– случайное нажатие клавиш на клавиатуре;

– случайный перебор пунктов меню программы.

1.3 Классификация и состав СКУД

Рассмотрим более подробно, что же представляет собой современная СКУД. Будем понимать под СКУД объединенные в комплексы электронные, механические, электротехнические, аппаратно–программные и иные средства, обеспечивающие возможность доступа определенных лиц в определенные зоны (территория, здание, помещение) или к определенной аппаратуре, техническим средствам и предметам (персональный компьютер (ПК), автомобиль, сейф и т. д.) и ограничивающие доступ лицам, не имеющим такого права. Такие системы могут осуществлять контроль перемещения людей и транспорта по территории охраняемого объекта, обеспечивать безопасность персонала и посетителей, а также сохранность материальных и информационных ресурсов предприятия.

В разделе 4 ГОСТ Р 51241–98 [4, п.4] дается следующая классификация СКУД:

1) по способу управления:
   - автономные – для управления одним или несколькими УПУ без передачи информации на центральный пульт и без контроля со стороны оператора;
   - централизованные (сетевые) – для управления УПУ с обменом информацией с центральным пультом и контролем и управлением системой со стороны оператора;
   - универсальные включающие функции как автономных, так и сетевых систем, работающие в сетевом режиме под управлением центрального устройства управления и переходящие в автономный режим при возникновении отказов в сетевом оборудовании, в центральном устройстве или обрыве связи;
2) по количеству контролируемых точек доступа:
   - малой емкости (менее 16 точек);
   - средней емкости (не менее 16 и не более 64 точек);
   - большой емкости (64 точки и более);
3) по функциональным характеристикам СКУД делятся на 3 класса:
   - 1 – системы с ограниченными функциями;

– 2 – системы с расширенными функциями;

– 3 – многофункциональные системы;

4) по виду объектов контроля:

– для контроля доступа физических объектов;

– для контроля доступа к информации;

5) по уровню защищенности системы от несанкционированного доступа к информации:

– нормальная устойчивость к разрушающим и неразрушающим воздействиям;

– повышенная устойчивость к разрушающим и неразрушающим воздействиям;

– высокая устойчивость к разрушающим и неразрушающим воздействиям;

6) по устойчивости к неразрушающим воздействиям СКУД делятся в зависимости от функционального назначения по следующим показателям:

– по устойчивости к вскрытию – для УПУ и исполнительных устройств (замков и запорных механизмов);

– по устойчивости к манипулированию;

– по устойчивости к наблюдению – для УВИП с запоминаемым кодом;

– по устойчивости к копированию (для идентификаторов);

– по устойчивости защиты средств вычислительной техники УУ от несанкционированного доступа к информации.

При этом классификацию СКУД по защищенности от несанкционированного доступа к информации проводят по **Ошибка! Источник ссылки не найден.**, а по у стойчивости от несанкционированного доступа к информации – по Таблица 4.

Таблица 3 – Требования к автоматизированным системам по группам

Подсистемы и требования	Группы и классы				
	3		2	1	
	3Б	3А	2Б	1Г	1В
1. Подсистема управления доступом					
1.1. Идентификация, проверка подлинности и контроль доступа субъектов. – в систему	+	+	+	+	+
– к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	–	–	–	+	+
– к программам	–	–	–	+	+
– к томам, каталогам, файлам, записям, полям записей	–	–	–	+	+
1.2. Управление потоками информации	–	–	–	–	+
2. Подсистема регистрации и учета					
2.1. Регистрация и учет: – входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+
– выдачи печатных (графических) выходных документов	–	+	–	+	+
– запуска/завершения программ и процессов (заданий, задач)	–	–	–	+	+
– доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	–	–	–	+	+
– доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	–	–	–	+	+
– изменения полномочий субъектов доступа	–	–	–	–	+
– создаваемых защищаемых объектов доступа	–	–	–	–	+
2.2. Учет носителей информации	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	–	+	–	+	+
2.4. Сигнализация попыток нарушения защиты	–	–	–	–	+
3. Подсистема обеспечения целостности					
3.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+
3.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+
3.3. Наличие администратора (службы) защиты информации в АС	–	–	–	–	+
3.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+
3.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+
3.6. Использование сертифицированных средств защиты	–	+	–	–	+
Примечание. Знак «+» означает наличие требования к данному классу, знак «–» – отсутствие требования к данному классу.					

Таблица 4 – Показатели защищенности от НСД к информации

Наименование показателя	**Класс защищенности**		
	6	**5**	**4**
1. Дискреционный принцип контроля доступа	+	+	+
2. Мандатный принцип контроля доступа	–	–	+
3. Очистка памяти	–	+	+
4. Изоляция модулей	–	–	+
5. Маркировка документов	–	–	+
6. Защита ввода и вывода на отчуждаемый физический носитель информации	–	–	+
7. Сопоставление пользователя с устройством	–	–	+
8. Идентификация и аутентификация	–	–	+
9. Гарантии проектирования	–	+	+
10. Регистрация	–	+	+
11. Целостность КСЗ	–	+	+
12. Тестирование	+	+	+
13. Руководство пользователя	+	=	=
14. Руководство по КСЗ	+	+	=
15. Тестовая документация	+	+	+
16. Конструкторская (проектная) документация	+	+	+
Примечание. Знак «–» означает отсутствие требования к данному классу, знак «+» – наличие новых или дополнительных требований, знак «=» – требования совпадают с требованиями СВТ предыдущего класса.			

В общем виде можно предложить такую логическую схему построения любой СКУД (см. Рисунок 1).

Рисунок 1 – Общая логическая схема построения СКУД

Остановимся подробнее на стандартных компонентах СКУД:

– контроллеры хранят в себе коды и права доступа (или запрашивают у баз данных, которые находятся на главном сервере), по сути, они решают, кого пропускать;

– идентификаторы представляют из себя устройства, которые необходимы для определения прав того, кто желает попасть на объект; могут быть исполнены в виде карточек, брелоков, современные системы могут использовать в качестве идентификатора радужку глаза, отпечатки пальцев, часть генетического кода;

– считыватели являются, можно сказать, посредниками между идентификатором и контролером, так как передают информацию от одного другому; исполнение зависит от идентификатора, например при считывании радужки глаза необходима специальная видеокамера);

– исполнительные (преграждающие) устройства (то, что будет препятствовать свободному доступу пользователей; для дверей это – электрозащелки, электромагнитные или электромеханические замки, для проездов или проходов – ворота, шлагбаумы, турникеты, дорожные барьеры);

– компьютеры или автоматизированные рабочие места, являются основными центрами взаимодействия с системой в любой современной СКУД, благодаря им возможно, во–первых, организовать единый пункт управления, контроля и

конфигурирования параметров системы, во–вторых, организовать базу данных для сбора событий системы с целью последующего анализа при возникновении инцидентов безопасности, в–третьих, с помощью локальной сети несколько компьютеров с программным обеспечением СКУД позволяют гибко распределять роли в системе и тем самым реализовать дополнительный функционал, полезный для других подразделений предприятия, например, учет рабочего времени сотрудников для табельщиков.

Обобщенно–усредненный алгоритм работы любой СКУД таков:

1) У входа на территорию, объект или помещение устанавливается устройство идентификации (считыватель). Он может быть представлен дверью с электрическим или другим типом замка, шлагбаумом (парковки) или турникетом с сопутствующим типом считывателя. Сегодня большинство СКУД все еще используют идентификаторы в виде карт или брелоков, которые привязываются к конкретному пользователю.

То есть, для доступа с их помощью потребуется приложить устройство к специальной панели или же провести картой. Крупные компании, которым важна защита информации, прибегают к приобретению СКУД с современными способами аутентификации: сканирование радужной оболочки глаз или лица человека посредством камеры, сканер отпечатка пальца и другое.

Стоимость таких систем высокая, но безопасность обеспечивается на максимальном уровне. Нередко способы идентификации совмещаются (многофакторная аутентификация).

2) Получив идентификационные данные пользователя, в работу вступает контроллер. Он, сверяя информацию, обращается к базам, в которых она и хранится. Контроллер выясняет, разрешен ли доступ конкретному пользователю, а также проверяет его права на вход в каждую из дверей (или ворот, или турникетов).

3) Если доступ разрешен, то контроллер посылает сигнал преграждающему устройству (замку), которое открывается, о чем может свидетельствовать звуковой или световой сигнал. В противном случае (доступ закрыт или ограничен) дверь останется закрытой, уведомив посетителя о невозможности

прохода.

Контроллеры, помимо того, что посылают сигнал на открытие или закрытие преграждающих устройств, могут быть запрограммированы на различные дополнительные действия. Например, некоторые фирмы разграничивают своих работников, предоставляя права доступа к определенным помещениям только ряду сотрудников – остальные войти не смогут.

Часто СКУД используется, чтобы обеспечить доступ на территорию только в заданный алгоритмом контроллеру промежуток времени. Система может быть запрограммирована таким образом, что сотрудник или посетитель сможет войти в помещение только в присутствии более привилегированного пользователя. Современные системы контроля и управления доступом поддерживают не один десяток режимов входа/выхода.

1.4 Обзор существующих решений СКУД

Для каждого промышленного предприятия всегда характерны уникальные особенности, связанные со спецификой его деятельности и внутренней организационной и технической структурой. Это порождает многообразие условий и требований к системам безопасности, и в частности, к СКУД. Поэтому на сегодняшний день существует множество производителей и совершенно разнообразных технологий, средств и систем безопасности, как отдельных компонентов, из которых можно собирать системы, так и полностью законченные решения «под ключ». Рассмотрим некоторые решения ведущих производителей систем безопасности специально для крупных промышленных предприятий

Для большого предприятия характерны такие особенности организации СКУД:

– Территориальная удаленность различных корпусов предприятия.

Для крупного предприятия характерно распределение отдельных составляющих по территории, что может повлиять на требования к СКУД. Так удаление непосредственного рабочего места от проходной может потребовать гибкого учета рабочего времени.

– Пиковые нагрузки на проходных в начале и конце рабочих смен.

Во избежание заторов на проходной предприятия необходимо тщательно подбирать количество турникетов, а также метод идентификации.

– Разноплановое оборудование для организации транспортного КПП.

В зависимости от особенностей проезжающего на предприятие транспорта (грузовые/легковые) необходимо обеспечить удобство самого процесса доступа, а также учет сотрудников прибывающих через КПП на корпоративном транспорте (например, автобус).

– Интеграция.

Большое количество используемых информационных систем и различного оборудования требует возможности объединять их в единую систему для повышения эффективности текущих бизнес–процессов.

При проектировании СКУД на крупном предприятии прежде всего целесообразно ставить такие цели:

– Повышение уровня безопасности объекта за счет ограничения доступа на территорию посторонних лиц;

– снижение внутренних угроз, за счет разграничения прав доступа в отдельные сектора/помещения объекта;

– автоматизация пропускного режима для людей и транспорта.

1.5 СКУД от SIGUR

Компания ПромАвтоматика, разработчик и производитель Sigur, присутствует на рынке СКУД с 2006 года. Сегодня компания входит в тройку крупнейших отечественных разработчиков систем контроля и управления доступом.

Под брендом Sigur производится система контроля доступа, линейка сетевых контроллеров СКУД, преобразователи интерфейсов и другое сопутствующее оборудование.

При разработке продукции компания стремится использовать в своих решениях последние технологические тенденции отрасли, такие как NFC, биометрия, защищенная идентификация, распознавание лиц и многие другие.

Рассмотрим решение компании для крупного промышленного предприятия. Схема оборудования проходной представлена на Рисунок 2.

Рисунок 2 – Схема проходной

Логика работы проходной такова. Постоянный сотрудник проходит через турникет после положительного результата идентификации. Посетитель должен сначала получить пропуск после предъявления необходимых документов в бюро пропусков, расположенном на территории проходной или недалеко от нее.

Использование программных модулей Sigur «Расширенная поддержка пропусков посетителей» и «Распознавание документов» позволяет автоматизировать выдачу временного пропуска от момента создания и согласования заявки на посещение до момента выдачи пропуска. Вся информация об истории выдачи временных пропусков, посетителях и их проходах регистрируется в СКУД.

При повторном посещении выдача пропуска может происходить по уже имеющимся данным посетителя без необходимости их повторного ввода в систему.

Сбор временных пропусков осуществляется автоматически при выходе с территории через турникет с картоприемником, куда посетитель обязан опустить пропуск, чтобы покинуть территорию.

Контроллеры Sigur (Рисунок 3) поддерживают полноценное управление любыми турникетами и другими исполнительными устройствами, учитывая все особенности моделей разных производителей.

Это обеспечивает корректную работу устройства в составе СКУД, а также гарантирует регистрацию всех событий: совершенных проходов (с указанием направления), отказов в доступе, взломов системы, действий, произведенных охранником вручную с пульта и других.

Для исключения ошибок монтажа Sigur предоставляет готовые схемы подключения к СКУД большинства популярных моделей исполнительных устройств разных производителей.

Рисунок 3 – Контроллер Sigur

Помимо поддержки любых считывателей со стандартным выходным интерфейсом Wiegand, в том числе и биометрических, в Sigur реализована глубокая интеграция со считывателями отпечатков пальца и вен ладоней «BioSmart» (производитель – ООО «Прософт–Биометрикс»), а также считывателями радужной оболочки глаза EyeLock.

Это позволяет в рамках программного интерфейса Sigur вносить в систему шаблоны, по которым производится распознавание, т.е. производить все необходимые настройки без использования нескольких программ.

Для повышения уровня безопасности можно использовать многофакторную идентификацию, т.е. два или больше признаков одновременно. В их числе могут быть: бесконтактные карты, отпечатки пальцев, распознанное лицо, рисунок вен ладоней, пин–код, штрих–код и другие.

В Sigur поддерживаются все перечисленные способы идентификации в различных комбинациях.

Рисунок 4 – Считыватель Sigur

В зависимости от бюджета и пожеланий заказчика Sigur предлагает различные варианты автоматизации процесса работы с посетителями и пропусками.

В Sigur реализованы:

– модуль работы с посетителями – для создания и согласования заявок на посещение и предварительного ввода персональных данных,

– сканирование и распознавание документов – для быстрого ввода паспортных данных посетителя,

– интеграция с терминалом выдачи пропусков VisitorControl – для полной автоматизации процесса выдачи пропусков без участия оператора

– интеграция с популярными моделями картоприемников, позволяющая тонко настраивать различные параметры их работы – для автоматического сбора временных карт и/или пропусков с истекшим сроком действия на выходе с территории.

Помимо этого в Sigur реализована интеграция с популярной системой регистрации, учета и контроля посетителей Visitor Control, что позволит настроить эффективное взаимодействие обеих систем в рамках одного объекта.

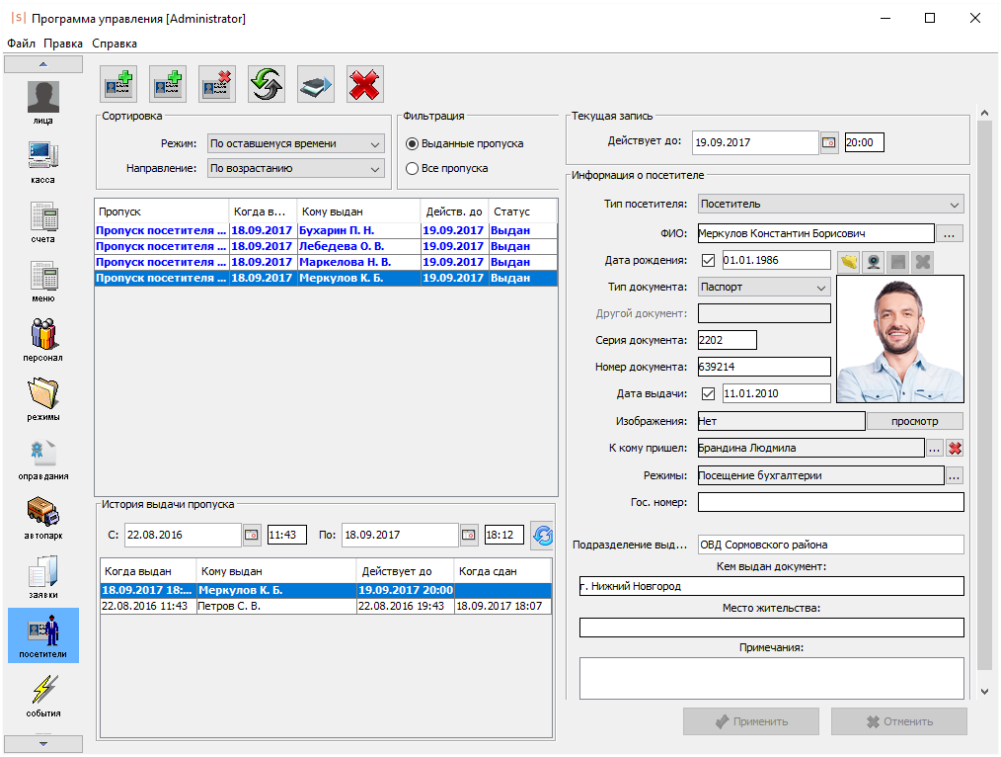

Рисунок 5 – АРМ бюро пропусков в SIGUR

На Рисунок 6 приведена схема КПП. Логика работы КПП в решении SIGUR построена следующим образом. Автотранспортное КПП предприятия состоит из 2 шлагбаумов, установленных на въезд и выезд и расположенных рядом. Каждый шлагбаум дополняется 3мя фотопарами, расположенными перед стрелой, под стрелой и после шлагбаума для определения направления проезда транспортных средств.

Наряду с каждым шлагбаумом к контроллеру Sigur подключаются светофоры для регулирования потока проезжающих с обеих сторон.

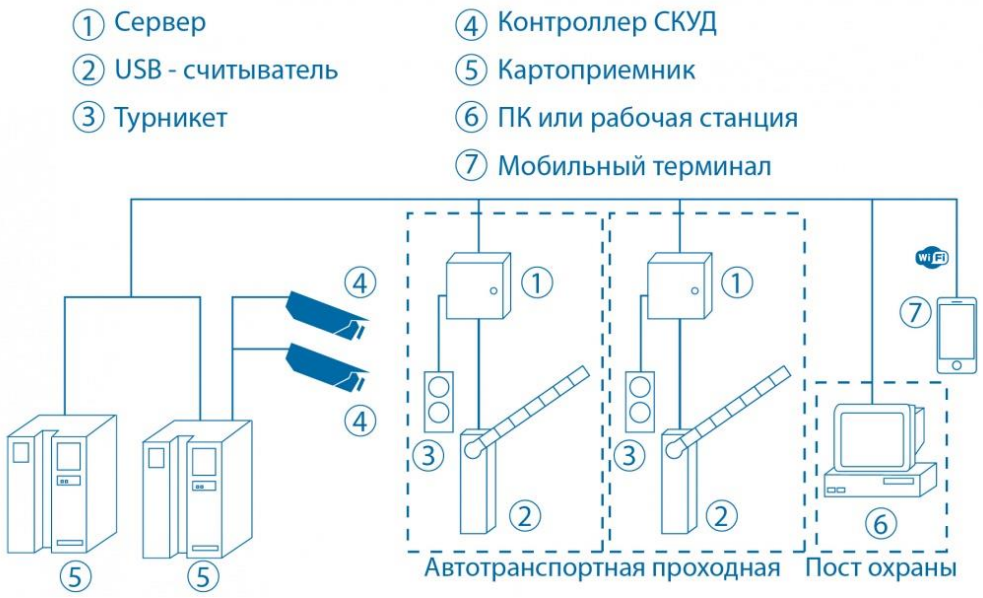

Рисунок 6 – Схема КПП

Въезд и выезд как постоянных, так и временных сотрудников осуществляется на основании распознавания номера транспортного средства. Реализация данного способа осуществляется при помощи интеграции с СВН Trassir, имеющей в составе модуль распознавания автомобильных номеров и видеокамеры.

Рядом с зоной проезда располагается пост охраны, включающий клиентское место Sigur с необходимым ПО. При возникновении нештатных ситуаций охранник может поднять/опустить шлагбаум сигналом с пульта или из интерфейса Sigur, все события при этом будут протоколироваться в системе.

Поскольку при автоматизации проезда используется распознавание номеров, считается, что для доступа во внутренние помещения сотрудники имеют другие идентификаторы, например бесконтактные карты. Если у а/м и сотрудника разные идентификаторы (государственный номер для проезда а/м и карточка сотрудника для прохода во внутренние помещения) то модуль “Автопарк” позволит установить соответствие между сотрудниками и их личными/служебными автомобилями, а также работать с путевыми листами.

В случае проезда автотранспорта, поставленного в соответствие сотруднику, через точку доступа, на посту наблюдения происходит отображение информации не только об автомобиле (гос.номер, модель, фотография и пр.), но и о самом сотруднике. Любой въезд/выезд автомобиля регистрируется СКУД не только как

факт проезда транспортного средства, но и как факт пересечения границы территории сотрудником, которому сопоставлен данный автомобиль.

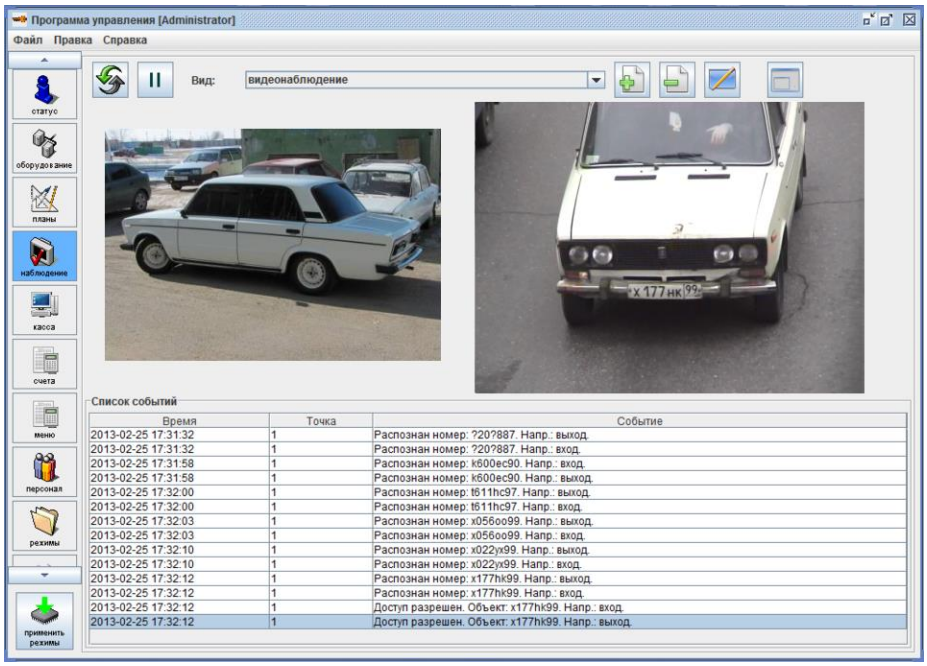

Рисунок 7 – Модуль «Автопарк» в SIGUR

При использовании корпоративного транспорта для доставки персонала к месту работы на КПП может использоваться мобильный терминал Sigur для регистрации сотрудников, въехавших на территорию на корпоративном автобусе.

В Sigur поддерживается подключение любых преграждающих устройств в различных комбинациях, например для повышения уровня безопасности совместно со шлагбаумами могут подключаться болларды или барьеры. Наряду с преграждающими устройствами контроллером Sigur поддерживается подключение различных датчиков и светофоров.

Рисунок 8 – Внешний вид КПП на основе оборудования SIGUR

Все возможные логики управления преграждающими устройствами реализованы в явном виде за счет загрузки всех управляющих линий. При этом алгоритм реализуется на контроллере аппаратно, что обеспечивает стабильную работу даже при отсутствии связи с сервером.

При необходимости использования дополнительных средств контроля в Sigur возможна интеграция с любыми досмотровыми или весовыми системами.

В Sigur каждому сотруднику или группе можно настроить не только диапазоны времени разрешенного входа и выхода через заданные точки доступа, но и правила прохода, включающие:

- доступ с санкции охраны;
- доступ только вдвоём;
- доступ с пин–кодом;
- доступ в сопровождении;
- доступ по правилу гос.номер плюс карта – для идентификации автотранспорта при автоматизации проезда;
- доступ по результатам алкотестирования, включающий настройку вероятности тестирования, максимально допустимую концентрацию и

возможность допуска при наличии паров этилового спирта в выдохе и другие параметры.

Sigur практически все сложные логики доступа реализованы на контроллере, что гарантирует стабильную работу системы.

При назначении правил доступа персоналу возможна настройка определенных условий, при которых они будут действовать, например, сотрудник, не прошедший технику безопасности, не будет допущен на рабочее место [10].

1.6 Решение от Parsec

Российская компания ООО «НПО Релвест», выпускающая свою продукцию под брэндом PARSEC, является разработчиком и производителем решений в области безопасности и идентификации объектов. Основными продуктами компании являются система контроля доступа ParsecNET, система дальней активной идентификации и оборудование для бесконтактной идентификации. Компания является одним из «пионеров» на российском рынке систем безопасности, выпуская продукцию под торговой маркой Parsec уже более 20 лет. Благодаря использованию в процессе разработки уникальных инновационных технологий наша компания считается признанным лидером отрасли.

Для обеспечения крупного предприятия с большим количеством сотрудников СКУД и УРВ разработано специальное решение СКУД ParsecNET 3. Открытая для интеграции платформа с широким набором сервисов, предоставляемых бесплатно, позволяет успешно создавать системы на базе исполнительных устройств разных производителей, в том числе модернизировать уже существующую проходную. Так, если на проходной предприятия уже установлено 3 турникета, можно дополнить их контроллерами и считывателями Parsec. Схема работы проходной представлена на Рисунок 9 – Схема .

Рисунок 9 – Схема проходной

Контроллеры NC–100K–IP (см. Рисунок 10 – были специально разработаны для работы с турникетами на проходных предприятий. Поддерживают одну двустороннюю или одностороннюю точку прохода. Контроллер подключается напрямую к сети Ethernet стандартным сетевым кабелем, для подключения которого плата контроллера снабжена стандартным Ethernet–разъемом (RJ–45).

Рисунок 10 – Контроллер NC–100K–IP

Среди возможностей контроллера, позволяющих наиболее полно обеспечить решение поставленных задач по организации проходной:

– увеличенные объемы базы данных пользователей и транзакций для обслуживания проходных крупных предприятий с численностью до 100 000 человек;

– с целью повышения скорости обмена с ПК и скорости загрузки работа только через высокоскоростной интерфейс Ethernet;

– два входа датчика дверного контакта (DC) или датчиков проворота турникета;

– программируемая полярность сигнала датчиков проворота турникета;

– поддержка дополнительного третьего считывателя с интерфейсом Wiegand для обслуживания картоприемника;

– отдельное реле для управления картоприемником;

– расширенный набор привилегий пользователей, в том числе: персональный запрет выхода через турникет, индивидуальный запрет выхода вне временного профиля, признак временного пользователя, признак гостевой карты для

пользователя;

– расширенные возможности контроллера, в частности: опциональное аппаратное удаление временных карт по истечении срока действия карты; запрет выхода вне временного профиля для любого пользователя; работа штатного внутреннего считывателя как считывателя картоприемника; опциональное аппаратное удаление гостевых карт после выхода с территории;

– ускоренная перезагрузка пользователей: полная загрузка всех пользователей при инициализации контроллера составляет порядка 10 минут.

Кроме того, контроллер NC–100K–IP поддерживает дополнительные возможности при работе с гостевыми картами:

– опциональное аппаратное удаление временных карт по истечении срока действия карты;

– запрет выхода вне временного профиля для любого пользователя;

– работа штатного внутреннего считывателя как считывателя картоприемника;

– опциональное аппаратное удаление гостевых карт после выхода с территории.

Помимо этого, в карточке посетителя, дополнительно можно указывать цель и дату визита, загружать изображение со сканера, камеры или фото из выбранной директории, а также вносить отметки о вносе или выносе материальных ценностей с объекта.

Считыватели PNR–EH15 (см. Рисунок 11 – Считыватель PNR–EH15) являются оптимальным решением для установки на турникетах и металлических поверхностях, так как корпус считывателя выполнен из цинка с гальваническим хромовым покрытием. Конструкция обеспечивает защиту от внешних механических повреждений и иных форм деструктивного девиантного поведения человека.

Считыватели предназначены для работы с низкочастотными (125 кГц) бесконтактными (proximity) картами EM Marin и HID Prox. Считыватели подключаются к контроллеру NC–100K–IP по трехпроводному протоколу Parsec. Это обеспечивает контроль состояния считывателя на линии, а также возможность

управления световой и звуковой индикацией, информирующей о состоянии точки прохода. При этом индикация RGB может быть настроена с помощью утилиты PNR_Tune.

Считыватель обеспечивает расстояние считывания для карт и брелоков от 10 до 50 мм в зависимости от их типа.

Рисунок 11 – Считыватель PNR–EH15

В крупных системах часто требуется иметь возможность подключения оборудования к нескольким ПК. Кроме того, обычно требуется организация нескольких рабочих мест одинакового или различного функционального назначения (рабочее сотрудника бюро пропусков, рабочее место охранника и так далее). В системе ParsecNET3 лицензируются модулем PNSoft–WS только консоли, то есть рабочие станции, на которых запускается пользовательский интерфейс. Для рабочих станций, которые занимаются только обслуживанием подключённого к ним оборудования, дополнительных лицензий не требуется.

Модуль бюро пропусков PNSoft–PO позволяет совместить функции работы, как с постоянными пропусками сотрудников, так и с разовыми пропусками посетителей, и организовать трёхзвенный процесс: подачи заявок на пропуска, утверждения (или отклонения) заявок и выдачи пропуска, если этот пропуск не бумажный.

При использовании на проходной картоприемников вместо обычных считывателей модуль также обеспечивает автоматическую фиксацию забора

пропуска у посетителя и возврат этого пропуска в пул свободных карт для повторного использования.

Бюро пропусков имеет свои шаблоны для печати пропусков, свои формы отчётов по результатам деятельности с различными критериями отбора.

При наличии модуля сканирования документов уровень автоматизации становится ещё выше — в таком случае отпадает необходимость ручного ввода данных о посетителе, причём в базу данных автоматически вводится даже фотография посетителя со сканируемого документа.

Для обеспечения пропуска автотранспорта крупного предприятия СКУД ParsecNET 3 специально разработан контроллер NC–8000, считывателя дальней идентификации PR–G07.N, а также активных меток ActiveTag.2 или ActiveTag.I2. Схема КПП представлена на Рисунок 12.

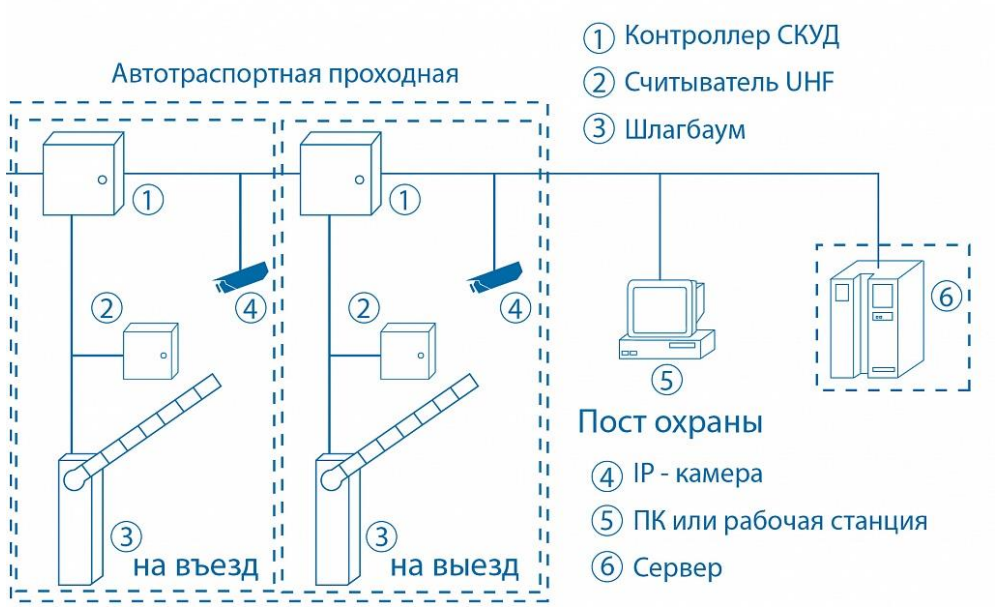

Рисунок 12 – Схема КПП

Контроллер NC–8000 предназначен для использования в составе системы ParsecNET. Каждый контроллер поддерживает оборудование одной точки прохода, а также систему охранной сигнализации помещения, связанную с данной точкой прохода. К выходам контроллера подключается замок (или любое другое устройство ограничения доступа, включая шлагбаумы и турникеты), а также исполнительное устройство системы сигнализации. Бесконтактный считыватель системы дальней идентификации PR–G07.N обеспечивает идентификацию

различных объектов, маркированных активными метками, на расстояниях от 5 до 50 и более метров. Заменяя два отдельных считывателя, PR–G07.N обеспечивает уникальные алгоритмы обработки идентификаторов, позволяющие разрешить конфликты в самых сложных вариантах применения.

Считыватель имеет два канала. Для каждого канала обеспечивается обработка принимаемых кодов меток, а также сигналов датчика автоматики ворот (шлагбаума) и датчика присутствия автомобиля, к каждому каналу подключается собственная антенна. Считыватель обеспечивает возможность как независимой, так и связанной работы каждого из каналов считывателя, как без датчиков автоматики, так и с любой их комбинацией.

Программные особенности считывателя, режимы работы:

– «Черный список» – запрет на вход и выход с отправкой соответствующей транзакции;

– «Запрет входа/выхода» – запрет идентификатору права на вход или на выход;

– возможность подсчета количества человек;

– возможность выдачи идентификаторов с лимитом использования по времени;

– возможность установки количества разрешенных проходов.

Из программных модификаций стоит отметить ряд полезных функций:

– восстановление состояния контроллера при потере питания;

– возможность задания расписаний для управления точкой прохода;

– установка максимального и минимального лимита человек, находящихся в помещении одновременно;

– проход по двум картам (проход с сопровождающим с использованием одного или двух считывателей);

– количество временных расписаний – 64, циклических – 64, праздничных дней – 32.

Для автоматизированного въезда–выезда машин из постоянного автопарка предприятия через КПП и учета рабочего времени сотрудников, прибывающих на

личном автотранспорте, в качестве идентификаторов идеально подходят активные метки ActiveTag.2, ActiveTag.I2 (см. Рисунок 13). Они выполнены в виде удобного брелока в пластиковом корпусе с двумя кнопками и линзой двухцветного светодиода. В комплекте также поставляется держатель, который может быть закреплен на плоской поверхности с помощью саморезов или двухсторонней липкой ленты. Идентификатор дополнительно имеет встроенную пассивную низкочастотную метку формата EM Marin, что позволяет использовать его и со стандартными считывателями систем доступа. Код метки EM Marin и код идентификатора, передаваемый по радиоканалу, совпадают, что позволяет использовать идентификатор для учета рабочего времени сотрудников предприятия.

Для фотофиксации и видеоверификации въезжающего можно установить IP–камеру [11].

Рисунок 13 –Активная метка ActiveTag.2

1.7 Решение от Smartec

Компания «СМАРТЕК СЕКЬЮРИТИ» занимается разработкой продукции в секторе профессионального оборудования для систем видеонаблюдения и контроля доступа. В активе компании представлены такие торговые марки, как Smartec и Alteron by Smartec. Схемы проходной и КПП представлены на Рисунок 14 – Схема проходной и Рисунок16 – Схема КПП.

Рисунок 14 – Схема проходной

Использование турникетов со встроенным контроллером и считывателем значительно упрощает процесс установки оборудования, а также повышает отказоустойчивость системы в случае выхода из строя одного из устройств турникетной группы.

Основная нагрузка на турникеты приходится час пик, поэтому расчет их количества осуществляется исходя из пропускной способности. Турникеты ST–TS101EM имеют проходную способность порядка 40 человек в минуту. Поэтому, чтобы избежать задержки более 10 минут, следует устанавливать 1 турникет на 350–400 человек.

Трехштанговый турникет ST–TS101EM (см. Рисунок 15 – Турникет ST–TS101EM) поставляется со встроенным контроллером ST–NC240 и считывателями карт EM для использования в составе системы контроля доступа под управлением

Таймекс.

Рисунок 15 – Турникет ST–TS101EM

Встроенная плата управления имеет 2 управляющих входа и 2 выхода сигнализации для использования с любой системой контроля доступа. Может быть реализована любая логика работы:

- регулируемый проход в обе стороны,
- регулируемый проход только в одну сторону
- свободный проход в обе стороны при разблокировке.

При замыкании выделенного управляющего входа или при потере питания преграждающая штанга падает автоматически и проход разблокируется для беспрепятственной эвакуации персонала в случае возникновения чрезвычайной ситуации.

Использование UHF считывателей позволяет обеспечить максимальное удобство пользователей при проезде через контрольно–пропускные пункты на автотранспорте. Схема проходной представлена на Рисунок 16 – Схема КПП

Контроллеры ST–NC120B, ST–NC240B и ST–NC440B (см. Рисунок 17 – Контроллер ST–NC120B) предназначены для построения современных и экономичных сетевых систем контроля доступа на базе программного обеспечения «Таймекс».

При включении в состав СКУД крупного предприятия обладают следующими

преимуществами:

– возможность автономной работы;

– энергонезависимая память до 100000 событий;

– до 30000 пользователей;

– совместимость с любыми считывателями (по интерфейсу Wiegand);

– дополнительные входы/выходы для мониторинга, например, датчиков охранной сигнализации или управления какими–либо устройствами в ручном или автоматическом режиме.

Рисунок 16 – Схема КПП

Считыватель ST–LR300 (см. Рисунок 18) с встроенной антенной предназначен для работы с UHF картами стандарта ISO–18000–6C, ISO–18000–6B и идеально подходит для решения задач, где требуется большое расстояние считывания, например, для контроля доступа автомобильного транс порта.

Рисунок 17 – Контроллер ST–NC120B

При включении в состав автомобильного КПП крупного предприятия обладают следующими преимуществами:

– настраиваемые расстояние считывания до 10 м, расстояние записи до 6 м;

– использование высокопроизводительного радиочипа R2000 с улучшенной фильтрацией;

– одновременное считывание до 100 идентификаторов;

– комплектуется кронштейном крепления на столбе;

– звуковая индикация;

– программируемый релейный выход;

– влаго/пылезащищенный корпус [12].

Рисунок 18 – Считыватель ST–LR300

1.8 Существующий уровень автоматизации

На предприятии в настоящее время практически завершено внедрение проекта СКУД на основе ИСО «Орион», поэтому в своей работе я делаю допущение, что данную СКУД можно считать существующим уровнем автоматизации. Программно–аппаратный комплекс СКУД на основе ИСО «Орион» детально будет рассмотрен в второй главе, пока лишь перечислим реализованный функционал системы:

1) контроль доступа:

– доступ в охраняемые зоны при помощи Proximity–карт;

– возможность использования одной и той же Proximity–карты для взятия под охрану/снятия с охраны и управления доступом;

– централизованное (в базе данных на сервере) и распределенное (в контроллерах) хранение ключей доступа;

– ограничение доступа по дате и времени;

– энергонезависимый календарь;

2) сбор и обработка информации:

– долговременное хранение информации о событиях с возможностью последующей расшифровки и анализа;

– комплексное предоставление информации оперативному дежурному и ответственным лицам;

– разграничение полномочий ответственных лиц при принятии решений и доступу к информации;

– наличие гибкой системы отчетности с широким набором шаблонов;

– поддержка интерфейсов для взаимодействия с внешними системами (данная возможность была использована в этой работе).

На сегодняшний день уровень развития технологий позволяет реализовывать СКУД, роль человека в которых стремительно снижается, что позволяет говорить о таких системах, как об автоматизированных системах контроля и управления доступом. Все более доступными и популярными становятся технологии

бесконтактной и биометрической идентификации: по отпечаткам пальцев, сетчатке глаза, по лицу. Использование подобных решений оправданно, поскольку уменьшается вероятность человеческой ошибки в процессе идентификации и одновременно повышается скорость принятия решения о допуске субъекта, что особенно актуально на средних и крупных предприятиях, где в начале и конце рабочего дня поток сотрудников, пропускаемых через проходные, может составлять до нескольких сотен человек за раз.

Несмотря на то, что ИСО «Орион» имеет варианты реализации с использованием средств биометрической идентификации, в рамках внедрения на предприятии такие возможности использованы не были, что послужило толчком к работе над проектом программного модуля распознавания лиц.

1.9 Технологии машинного зрения в современных СКУД на промышленном предприятии

1.9.1 Особенности внедрения и использования систем контроля доступа по лицу: преимущества и сложности

Биометрические технологии идентификации личности находят все более широкое применение в СКУД. На сегодня традиционные способы идентификации личности, в основе которых находятся разные идентификационные карты, ключи или уникальные данные, не являются надежными в той степени, которая необходима. Биометрическое опознание производится не по присвоенным человеку идентификационным признакам, а по физиологическим свойствам или особенностям самого человека – уникальной персональной информации, которую не нужно держать в памяти, невозможно потерять и имитация которой крайне затруднительна.

На таком объекте как Челябинское ЛПУМГ, являющимся стратегически важным для топливно-энергетического комплекса России, необходим наивысший уровень безопасности и безусловным приоритетом здесь служит надежность идентификации сотрудников. Очевидно, что в СКУД таких объектов применение биометрии не только возможно и желательно, но и жизненно необходимо. Среди всех биометрических технологий здесь на первый план выходят технологии, обеспечивающие наименьший уровень ошибок FAR (идентификация по отпечаткам пальцев, радужной оболочке глаз и др.), и технология распознавания по лицу используется как одна из составляющих мультибиометрических решений.

Другим преимуществом применения распознавания по лицу является пропускная способность СКУД, когда малейшая задержка в процессе идентификации и пропуска сотрудника способна парализовать функционирование всего объекта или его структурного элемента. В этом случае технология распознавания по лицу является наиболее предпочтительным, а зачастую и единственным решением, поскольку бесконтактный способ распознавания не требует от сотрудников никаких дополнительных действий (доставания и

предъявления пропуска, прикладывания карты к считывателю и т.п.), а значит – и затрат времени на эти действия.

Третьим преимуществом использования технологии идентификации по лицу является простота применения для проходящего сотрудника. Человек, характеристики которого сканируются, не должен при этом испытывать никаких неудобств.

Как и все биометрические технологии, распознавание по лицу является вероятностной и не способна гарантировать полное отсутствие ошибок FAR/FRR, то есть коэффициентов ложного пропуска (False Acceptance Rate – система предоставляет доступ незарегистрированному пользователю) и ложного отказа в доступе (False Rejection Rate – доступ запрещен зарегистрированному в системе человеку). Однако в последнее время эта технология находит все более широкое применение.

На сегодня используются две основные технологии распознавания лиц – по геометрии лица (2D-технологии), в основе технологии лежат плоские, или двухмерные, изображения и по строению черепа (3D-технологии), в которых распознавание производится по реконструированным трехмерным образам.

3D-технологии пока не получили широкого применения. Дороговизна и громоздкость оборудования, невысокая скорость идентификации, отсутствие возможности обслуживать большое число пользователей в режиме идентификации – вот далеко не полный перечень тех факторов, которые не позволили 3D-технологиям распознавания лиц массово выйти на потребительский рынок.

Вместе с тем 2D-технологии значительно распространены и позволяют осуществлять распознавание дистанционно, без непосредственного контакта посетителей с оборудованием, а при использовании соответствующего оборудования анализ информации может осуществляться с приемлемой скоростью. Источниками данных для биометрической идентификации способны выступать фотографии людей, результаты видеонаблюдения, другие видеозаписи. Однако системы 2D-распознавания очень чувствительны к изменениям идентификатора (появление очков, бороды и т.д.) и внешним факторам (поворот головы, освещенность и т.п.). Именно на снижение чувствительности системы к

изменениям идентификатора и на снижение влияния внешних факторов направили все свои усилия производители современных систем распознавания по лицу.

Как и любая биометрическая система, распознавание по лицу начинается со сканирования объекта. В качестве сканеров лица могут выступать как автономные сканеры, так и сканеры с подключением к централизованному серверу.

Автономные сканеры лица, как правило, подключаются к контроллерам СКУД, с помощью которых обеспечивается управление исполнительными устройствами. Поскольку вычислительные возможности таких устройств весьма ограничены, то для распознавания используются довольно простые алгоритмы, что приводит к значительному числу ошибок FAR/FRR. К тому же сформированный шаблон изображения создается в самом устройстве, что значительно снижает возможность масштабирования системы, поскольку каждый автономный сканер необходимо настраивать в отдельности. Применение сканеров, подключаемых к централизованному серверу, предпочтительнее, но и здесь существует ряд нюансов, которые необходимо учитывать.

В качестве сканеров лица зачастую используют обычные видеокамеры, расположенные на объекте, и здесь сразу же появляется проблема неправильного размещения камеры. Если устройство размещено под значительным углом к распознаваемому лицу, то число ошибок FAR/FRR возрастает, а если же камера размещена непосредственно на пути следования распознаваемых, то необходимо исключить возможность случайного физического контакта с камерой, в результате которого настройки положения видеокамеры будут сбиты.

Другой проблемой является недостаточная или неправильная освещенность лица. Необходимо обеспечить равномерное освещение в месте установки системы, избежав «засветки» от прямых солнечных лучей. Источник освещения следует располагать за видеокамерой на одной оптической оси. Смещение источника освещения в какую-либо сторону либо расположение его напротив камеры значительно снижают или же вовсе исключают возможность правильного распознавания лица.

Еще одна проблема заключается в том, как заставить проходящего человека смотреть именно туда, куда нужно. Применяемое в таких системах 2D-

распознавание требует, чтобы человек смотрел именно в камеру, с минимальным отклонением от прямого угла между видеокамерой и лицом. Простейшим решением является размещение экрана, на котором пользователь видел бы самого себя и смог правильно позиционироваться относительно камеры. Бюджетной альтернативой при этом вполне может выступать зеркало с нанесенными на него маркерами позиционирования. Несомненным плюсом системы будет являться голосовое оповещение процедуры прохода на объект, если человек незнаком с работой системы, следует информировать его о том, что делать и куда смотреть. Звуковое сообщение, призывающее посмотреть на терминал, привлечет внимание проходящего человека и подскажет, что ему делать в дальнейшем. Оптимальным решением является моноблочное размещение освещения и видеокамеры на зеркальном экране с функцией звукового оповещения о последовательности действий, которое позволит позиционировать пользователя относительно камеры, заодно применить дополнительное освещение и подсказать проходящему человеку, что делать.

Обобщая изложенное выше, можно выделить такие ключевые параметры СКУД с распознаванием лица:

1 Время прохода через турникет.

Данный параметр имеет особое значение в тех случаях, когда численность персонала организации значительная. Длительный период распознавания будет создавать очередь перед проходной. Время прохода через турникет складывается из сканирования (оцифровки изображения), передачи изображения на сервер, получения шаблона, сравнения шаблона с полученным изображением, открытие турникета. Для комфортного времени прохода (1–1,5 с) необходимо обеспечить быстродействие всех без исключения операций. Одним из ключевых факторов, определяющих быстродействие системы, является применение Ethernet-технологий, облегчающих подключение устройств, масштабирование системы и обладающих высокой скоростью передачи информации. Использование протокола RS-485 для связи контроллеров СКУД не сможет обеспечить необходимое быстродействие системы в целом.

2 Процент распознавания лица.

Технология допуска по лицу в СКУД для легитимного применения должна иметь высокий процент распознавания. Обычно заказчик настаивает на проценте не ниже чем 99%. Обеспечить его без технических ухищрений обычно не представляется возможным – места установки камер отличаются друг от друга, освещение точек прохода разнится. В то же время если фото человека сделано одной камерой, то вероятность распознавания ею же обычно составляет не менее 99%. Поэтому рекомендуется хранить и использовать для распознавания адаптивные шаблоны лица для каждого человека и для каждой видеокамеры в отдельности.

Со временем лицо человека подвержено естественным изменениям. Разные прически, наличие усов или бороды делают человека менее узнаваемым для системы. Наиболее перспективно в этом плане применение адаптивных шаблонов лица FinePattern, которые автоматически модифицируются при небольших изменениях внешности человека. При этом в качестве шаблона используется не одно, а несколько изображений, худшее из которых автоматически заменяется на лучшее. Применение адаптивных шаблонов FinePattern позволяет обеспечивать высокую вероятность распознавания как при сезонных изменениях (наличие/отсутствие головного убора), так и при изменении физических характеристик лица: старение, появление бороды и усов, изменение прически.

Нельзя упускать из виду удобство добавления лиц в базу данных системы. Одним из наиболее эффективных способов является режим «обучения», при котором лицо попадает в базу данных автоматически, при первом поднесении карты к считывателю на проходной, а потом уже готовый шаблон используется для верификации человека и распознавания его на других проходных. При наличии этого режима внедрение системы аутентификации по лицу проходит без участия операторов бюро пропусков, инженеров обслуживающих организаций. Фактически система аутентификации внедряется автоматически. Инженеры, внедрявшие подобную систему, знают, насколько тяжело произвести фотографирование нескольких тысяч человек, обеспечив необходимый уровень качества фото, причем необходима 100%-ная явка сотрудников организации и прочие условия. При наличии в строящейся системе аутентификации режима «обучения» достаточно

просто выдать именные карты – и все.

3 Возможности оперативного расширения базы данных.

На крупном предприятии число сотрудников может достигать тысяч человек, при этом имеет место такое явление, как текучка персонала (регулярный прием и увольнение). В таких условиях критически важным является время, необходимое для подготовки и занесения в базу данных всех необходимых для распознавания по лицу данных о новом сотруднике и возможности быстрой обработки системой управления базами данных (СУБД) базы данных с числом записей в несколько тысяч. Увеличение численности пользователей в системе не должно отражаться на времени поиска и, как следствие, времени прохода, поэтому используемые в системе распознавания по лицу СУБД должны быть реализованы на основе Oracle или MS SQL Server [13].

1.9.2 Обзор решений с использованием технологии распознавания лиц

1.9.2.1 СКУД «СтилПост» от компании «Стилсофт»

На базе контроллеров СКУД с гибкой программируемой логикой работы и специализированного программного обеспечения компания «Стилсофт» предлагает масштабируемую СКУД «СтилПост», не зависящую от численности персонала, числа контролируемых зданий и помещений и имеющую все необходимые функции для управления безопасностью объекта.

СКУД «СтилПост» обеспечивает создание как классических, так и биометрических СКУД для отдельных и территориально удаленных объектов одного предприятия. «СтилПост» поддерживает все применяемые на данный момент устройства идентификации и аутентификации. Это и Proximity-считыватели, и различные виды сканеров: сканеры отпечатка пальца, штрихкода, магнитных карт, Touch Memory.

Используемая в «СтилПост» технология распознавания лиц FaceScan, разработанная компанией «Стилсофт», обеспечивает высокую (не менее 99%) вероятность распознавания лица. FaceScan обладает большой

производительностью, в результате чего проход через турникет типа «московское метро» осуществляется всего лишь за 1,5 с. В технологии распознавания лиц компании «Стилсофт» используются адаптивные шаблоны, которые позволяют осуществлять модификацию шаблона распознавания лица под каждое конкретное устройство видеоаутентификации, расположенное на предприятии. Использование адаптивных шаблонов позволяет обеспечивать высокую вероятность распознавания как при сезонных изменениях (наличие/отсутствие головного убора), так и при изменении физических характеристик лица: старении, появлении бороды и усов, изменении прически [14].

1.9.2.2 СКУД на базе биометрической системы идентификации личности «Каскад-Контроль»

Система «Каскад-Контроль» представляет собой решение по автоматизации биометрического контроля доступа, временного учета присутствия персонала на территории предприятия и отслеживания нарушений в режиме реального времени. СКУД позволяет вести непрерывный мониторинг и идентификацию личности людей, осуществляющих проход в контролируемую зону, по изображению лица, полученному с камер видеонаблюдения в режиме реального времени. Гибкие настройки алгоритмов принятия решения позволяют реализовать блокирование или разблокирование средств ограничения доступа (турникетов, э/м замков, калиток, ворот и т.д.) в зависимости от правила прохода в контролируемую зону, установленную и принятую регламентами для данной группы лиц. Режим наблюдения позволяет скрыто накапливать статистику и вести электронные журналы посещения с получением полной информации о проходе данного лица.

Основой системы является новейшая технология биометрического распознавания лиц «Каскад-Поиск», заключающаяся в автоматическом сопоставлении вычисленных по изображению лица признаков с базой данных биометрических шаблонов[15, 16].

1.10 Постановка цели и задач

Целью работы является разработка проекта модернизации существующей СКУД за счет добавления к ней функционала распознавания лиц на основе программного модуля с использованием библиотеки компьютерного зрения с открытым исходным кодом OpenCV от INTEL. Для достижения этой цели требуется решить следующие задачи:

1. Исследование существующих решений с использованием технологий распознавания лиц.
2. Изучение внедряемой на предприятии СКУД на основе ИСО «Орион».
3. Изучение алгоритмов распознавания лиц, предлагаемых библиотекой OpenCV.
4. Выбор оптимального алгоритма распознавания из доступных в библиотеке OpenCV.
5. Выбор метода взаимодействия со СКУД.
6. Разработка схемы модернизации на основе выбранного алгоритма распознавания и метода взаимодействия со СКУД.
7. Конфигурирование программного комплекса СКУД ОРИОН Про для взаимодействия с модулем распознавания лиц.
8. Разработка программного модуля распознавания лиц.

2. СКУД на основе ИСО «Орион» на предприятии Челябинское ЛПУМГ

2.1 Общая характеристика системы: возможности, технические данные и структура

Интегрированная система охраны «Орион» представляет собой совокупность аппаратных и программных средств для организации систем охранно–пожарной сигнализации, контроля доступа, видеонаблюдения, автоматического пожаротушения, а также для создания систем контроля и диспетчеризации объектов.

Система обеспечивает:

- сбор, обработку, передачу, отображение и регистрацию извещений о состоянии шлейфов охранной, тревожной и пожарной сигнализации;
- контроль и управление доступом (управление преграждающими устройствами типа шлагбаум, турникет, ворота, шлюз, дверь и т. п.);
- видеонаблюдение и видеоконтроль охраняемых объектов;
- управление пожарной автоматикой объекта;
- взаимодействие с инженерными системами зданий;
- модульную структуру, позволяющую оптимально оборудовать как малые, так и очень большие распределенные объекты;
- защищенный протокол обмена по каналу связи между приборами.

Производитель ИСО, НВП «Болид», определяет ИСО «Орион» как объединение нескольких локальных ИСО, подразумевая возможности сетевых контроллеров взаимодействовать между собой по протоколу RS–485. Это дает возможность развертывания до 127 локальных ИСО по территории предприятия.

Основные технические данные локальной ИСО «Орион» приведены в Таблица 1.

ИСО «Орион» строится по принципу трехуровневой модели: нижний, средний и верхний уровни (см. Рисунок 19) [18].

В рамках данной работы я буду рассматривать только локальную ИСО с оборудованием для системы контроля и управления доступом (далее именно это

будет подразумеваться под сокращением СКУД).

Вкратце функционал системы был описан в первой главе (пп. 1.5). Следует отметить, что наиболее значимые и сложные возможности системы реализованы при помощи программного обеспечения «Орион ПРО», установленного на АРМ системы. Собственно, благодаря функциям, предоставляемым этим программным комплексом и стал возможным проект распознавания лиц.

Таблица 5 – Основные технические данные локальной ИСО «Орион»

Количество приборов, подключаемых к линии интерфейса RS–485	до 127
Количество зон, объединяемых в разделы (АРМ «Орион Про»)	до 16 000
Количество зон, объединяемых в разделы (ПКУ «С2000М»)	до 2048
Количество разделов (АРМ «Орион Про»)	до 10 000
Количество разделов (ПКУ «С2000М»)	до 512
Количество точек доступа	до 254
Количество выходов для управления внешними устройствами (АРМ «Орион Про»)	до 16 000
Количество выходов для управления внешними устройствами (ПКУ «С2000М»)	до 255
Количество пользователей (АРМ «Орион Про»)	не ограничено
Количество пользователей (ПКУ «С2000М»)	до 2047
Длина линии интерфейса RS–485 (без использования дополнительных повторителей)	до 3 000

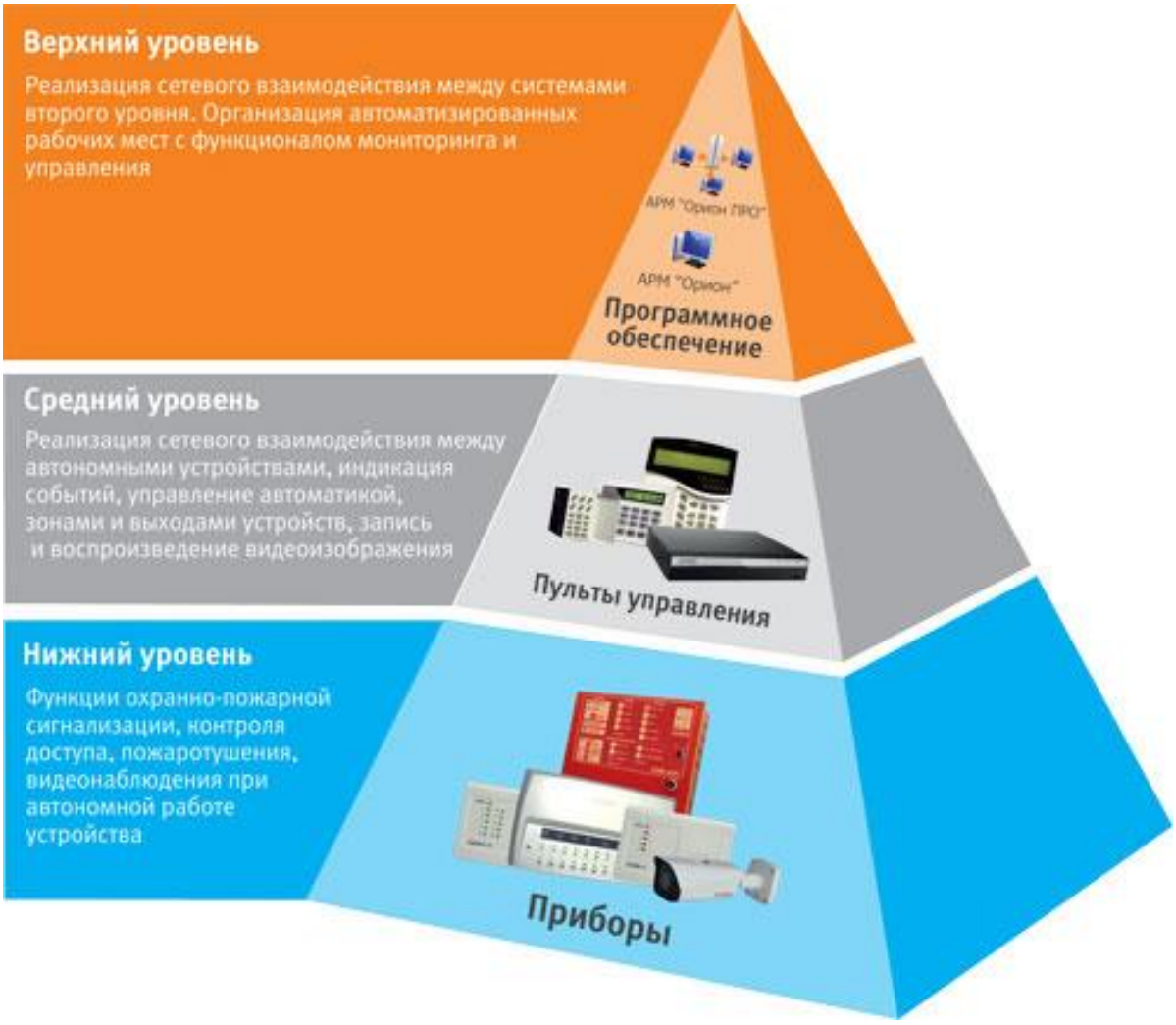

Рисунок 19 – Трехуровневая модель построения ИСО «Орион»

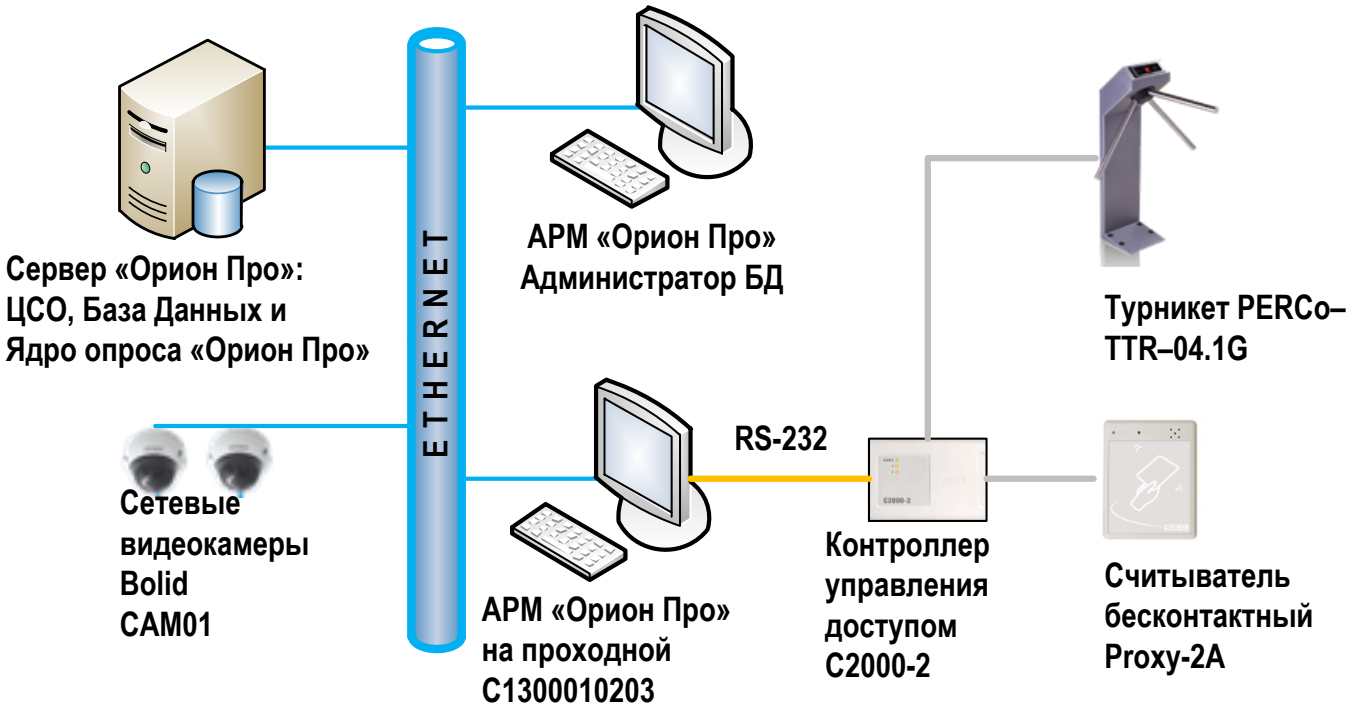

Рисунок 20 – Структурная схема СКУД

2.2 Оборудование СКУД

2.2.1 Контроллер доступа с2000–2

Предназначен для управления доступом через одну или две точки доступа путем считывания кодов предъявляемых идентификаторов (карт Proximity, ключей Touch Memory и PIN–кодов), проверки прав и ограничений доступа и замыкания (размыкания) контактов реле, управляющих запорными устройствами (электромеханическими и электромагнитными замками и защелками, турникетом, шлагбаумом). Предназначен для использования в составе системы «Орион» или автономно. Внешний вид контроллера представлен на Рисунок 21.

Рисунок 21 – Контроллер доступа с2000–2

Характеристики контроллера:

1) контроль одной точки доступа на вход и на выход или двух точек доступа на вход;
2) разнообразные режимы работы:
   - «Дверь на вход/выход»;
   - «Турникет»;
   - «Шлагбаум»;
   - «Шлюз»;
   - «Две двери на вход»;
3) подключение считывателей ключей Touch Memory, карт Proximity или PIN– кода с интерфейсом Touch Memory, Wiegand, ABA TRACK II и управление двухцветным светодиодом и звуковым сигнализатором считывателя;

4) режим запрета повторного прохода (Antipassback);
5) возможность управления взятием/снятием под охрану и доступом одной Proxymity картой или ключом Touch Memory;
6) настраиваемый контроль взлома и блокировки двери;
7) программируемый временной график доступа;
8) встроенные энергонезависимые часы с календарем;
9) двойная идентификация (Proximity карта + PIN– код);
10) доступ по правилу двух (трех) лиц;
11) доступ по коду принуждения (вер.2.20);
12) синхронизация работы нескольких контроллеров;
13) доступ с подтверждением кнопкой;
14) шлейфа охранной сигнализации (ШС1, ШС2);
15) возможность использования цепей подключения датчиков открывания двери в качестве ШС3, ШС4;
16) встроенный звуковой сигнализатор;
17) Управление и передача сообщений по интерфейсу RS–485 в ИСО «Орион»;
18) запоминание событий в буфере при потере связи по интерфейсу RS–485.

2.2.2 Считыватель бесконтактный PROXY–2A

Предназначены для считывания кода с идентификационных карточек и передачи его на приборы приемно–контрольные или контроллеры СКУД. В ИСО «Орион» используется для обеспечения процедур управления шлейфами и разделами охранно–пожарной сигнализации и идентификации пользователей в точках доступа СКУД. Характеристики прибора приведены в Таблица 6. Внешний вид представлен на Рисунок 22.

Таблица 6 – Характеристики считывателя бесконтактного PROXY–2A

НАИМЕНОВАНИЕ ПАРАМЕТРА	ЗНАЧЕНИЕ ПАРАМЕТРА
Дистанция считывания	До 12 см
Световая индикация	1 светодиодный индикатор питания 1 индикатор для отображения режимов работы считывателя
Внешний интерфейс	1 контактная колодка под винт для подключения к приборам
Интерфейс подключаемых приборов	Dallas Touch Memory RS –232 ТТЛ RS–232/DATA Wiegand–26, Wiegand–37, Wiegand–44 ABA TRACK II
Управление индикацией	1 светодиод READY (двухцветный красный–зеленый), управляемый, имеет две линии управления – красным и зеленым. 1 светодиод Power (оранжевый), неуправляемый Сигнал управления 5В TTL с возможностью выбора управления «активный 0» или «активная 1» с ограничением тока при прямом подключении светодиодов на уровне 10 мА
Встроенный звуковой сигнализатор	есть, управляемый
Питание прибора	от прибора, к которому подключен считыватель или от отдельного источника постоянного тока
Напряжение питания	8,0 ÷ 15,0 В
Потребляемый ток	не более 100 мА
	не более 160 мА
	не более 180 мА
Рабочий диапазон температур	от –25 до +60°С

Продолжение таблицы

НАИМЕНОВАНИЕ ПАРАМЕТРА	ЗНАЧЕНИЕ ПАРАМЕТРА
Относительная влажность	до 95%
Степень защиты корпуса	IP20
Габаритные размеры	123x97x14 мм
Масса	не более 90 г
Средний срок службы	10 лет
Тип монтажа	настенный врезной

Рисунок 22 – Считыватель бесконтактный PROXY–2A

2.2.3 Турникет PERCo TTR–04.1

Даная модель предназначена для эксплуатации внутри помещений. Компактная конструкция позволяет использовать турникет TTR–04.1 на проходных любой конфигурации. Внешний вид турникета представлен на Рисунок 23.

Управление турникетом возможно как от системы контроля доступа, так и автономно с помощью пульта дистанционного управления.

Режим работы — разрешение или запрет прохода — может быть задан независимо для каждого направления прохода. Встроенные в стойку турникета оптические датчики поворота преграждающих планок фиксируют реальный факт прохода и его направление, что обеспечивает корректный учет рабочего времени в

системах контроля доступа.

Плата блока управления конструктивно размещена в корпусе турникета. Механизм доворота обеспечивает автоматический доворот преграждающих планок до исходного положения после каждого прохода. Встроенный гидравлический демпфер обеспечивает плавную и бесшумную работу турникета.

Рисунок 23 – Турникет PERCo TTR–04.1

2.2.4 Камера сетевая VCI–212

Цветная камера предназначена для работы в составе комплекса видеонаблюдения и непрерывной трансляции видеоизображения с охраняемой зоны на системы отображения, записи, хранения и воспроизведения видеоизображения. Также возможна фотосъемка в высоком разрешении. Внешний вид камеры представлен на Рисунок 24.

Характеристики камеры:

- формат HD Ready с разрешением 1280×720 пикселей;
- кодек H.264;
- антивандальная защита класса IK10;
- водонепроницаемый пылезащищенный корпус с классом защиты IP67;
- встроенная ИК–подсветка;
- встроенный адаптер PoE для питания видеокамеры по кабелю сети Ethernet;
- расширенный динамический диапазон для одновременного отображения ярких и темных участков одного кадра;

– высокая чувствительность в условиях плохой освещенности [18].

Рисунок 24 – Камера сетевая VCI–212

2.3 Программное обеспечение СКУД «Орион Про»

АРМ «Орион Про» — пакет программного обеспечения для аппаратно–программного комплекса ИСО «Орион», на котором реализуются системы охранной сигнализации, контроля и управления доступом, охранного видеонаблюдения, автоматика противопожарных систем, сопряженные с инженерными системами объектов.

Программное обеспечение предназначено для организации компьютерных рабочих мест с целью повышения эффективности оперативного контроля и автоматизации управления системами, масштабирования ИСО «Орион», построения единых систем безопасности для территориально распределенных объектов, интеграции всех подсистем на программном уровне.

АРМ «Орион Про» может функционировать как на одном рабочем месте, так и на распределенных рабочих местах, объединенных через локальную вычислительную сеть. Для работы со СКУД пакет АРМ «Орион Про» включает в себя следующие программные модули: «Сервер» и «Администратор базы данных».

Основные показатели системы:

1) модульная архитектура и масштабируемость. Система состоит из отдельных функциональных модулей, с помощью которых возможно организовать полноценное автоматизированное рабочее место на одном компьютере, либо создать распределенную сеть рабочих мест, связанных по Ethernet или VPN–каналу. Каждый функциональный модуль за счет гибких настроек обеспечивает возможность специализации отдельно взятого рабочего места под

определенную задачу. Наращивание системы реализуется за счет приобретения дополнительных модулей уже и в процессе эксплуатации;

2) возможность конфигурирования каждого функционального модуля персонально позволяет реализовать конкретную специализацию каждого рабочего места под определенную задачу, программирование сценариев управления с помощью встроенного языка, поддержка наращиваемости определяют способность системы функционировать в соответствие с особенностями и спецификой охраняемого объекта;

3) отказоустойчивость комплекса обеспечивается за счет поддержки функционирования локальных рабочих мест с «Оперативной задачей» после потери связи с сервером системы. Поддержка горячего резервирования центрального сервера системы. Данный механизм основан на реплицировании базы данных в MS SQL.

2.3.1 Центральный Сервер системы «Орион Про» (ЦСО)

Работа системы начинается с запуска ЦСО. Этот программный модуль должен быть запущен постоянно. Только ЦСО работает непосредственно с Базой данных (далее — БД) АРМ «Орион Про», передаёт всем прочим модулям информацию из БД и заносит в БД изменения настроек системы, новые события и т.д.

В случае нескольких объединенных сетью АРМ, ЦСО необходим для взаимодействия всех сетевых АРМ с базой данных (MS SQL Server 2005/ 2008/2012).

2.3.2 Администратор базы данных «Орион Про»

Функции модуля для СКУД:

- создание базы данных СКУД;
- конфигурирование логических объектов охраны, таких как: зона, раздел, группа разделов, точка доступа, зона доступа;
- формирование базы данных «Бюро пропусков»: создание списка

сотрудников с указанием для каждого человека всех необходимых атрибутов: личные данные, информации о принадлежности к подразделению и фирме. Возможность изменения названий полей в форме отображения данных сотрудника;

– создание полномочий СКУД, ограничение управления с помощью задаваемых администратором полномочий для выданных ключей и паролей;

– прописывание полномочий доступа в контроллеры в режиме реального времени, а также обновление данных о СКУД на рабочих местах без общей перегрузки базы данных;

– формирование базы данных «Учета рабочего времени»: график работы, правила расчета графика работы для сотрудника и подразделений;

– программирование сценариев управления с помощью шаблонов и специального встроенного языка программирования «Орион – Скрипт»;

– настройка автоматической реакции системы на любые события;

– возможность регистрации информации о посетителях, задания правил управления доступом;

– регистрация нарушителей.

В разделе «Доступ» создаются логические объекты и структура системы контроля доступа:

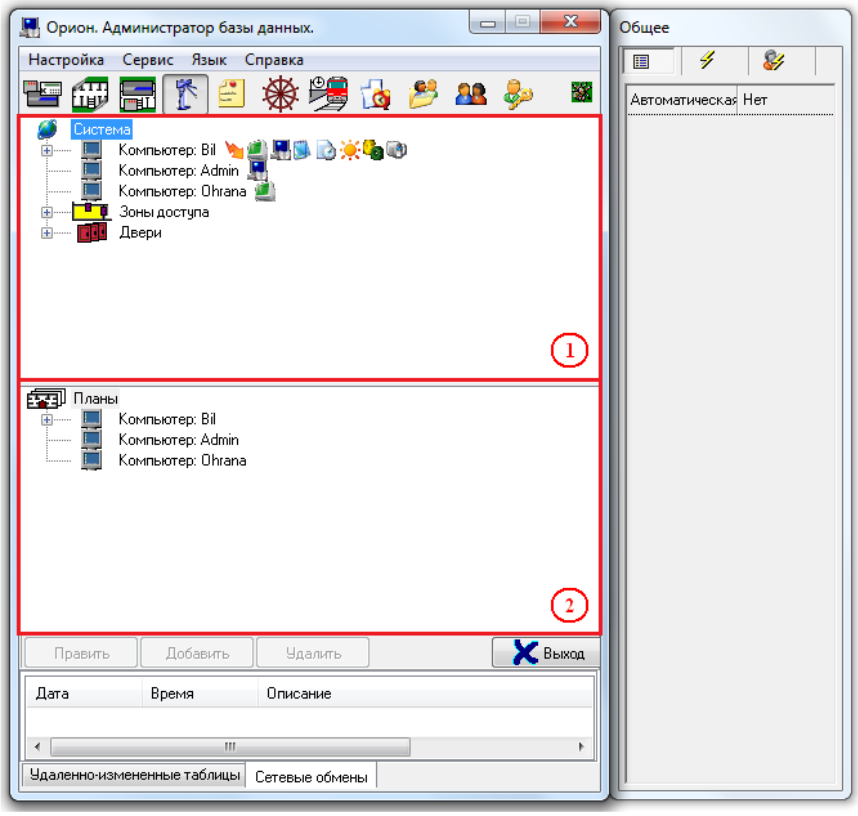

Рисунок 25 – Интерфейс модуля Администратор базы данных «Орион Про». Раздел «Доступ»; 1 – дерево объектов системы контроля доступа; 2 – дерево планов помещений

В разделе «Сценарии управления» создаются и настраиваются микропрограммы, выполняющие определённые действия (в основном посылают команды объектам системы), называемые сценариями управления. Сценарии управления могут быть:

1) созданы на основе шаблонов (в этом случае, сценарий управления — это набор последовательных шагов, каждый из которых выполняет определённое действие);

2) написаны на специально разработанном макроязыке сценариев (в этом случае, сценарий управления — это программа на макроязыке сценариев).

Сценарии управления могут запускаться:

3) оператором программного модуля «Монитор системы»:

– при помощи «горячих» клавиш;

– при помощи дерева управления;

4) автоматически по расписанию;

5) автоматически при возникновении в системе каких–либо событий. Именно такой способ и был задействован в проекте с распознаванием лиц.

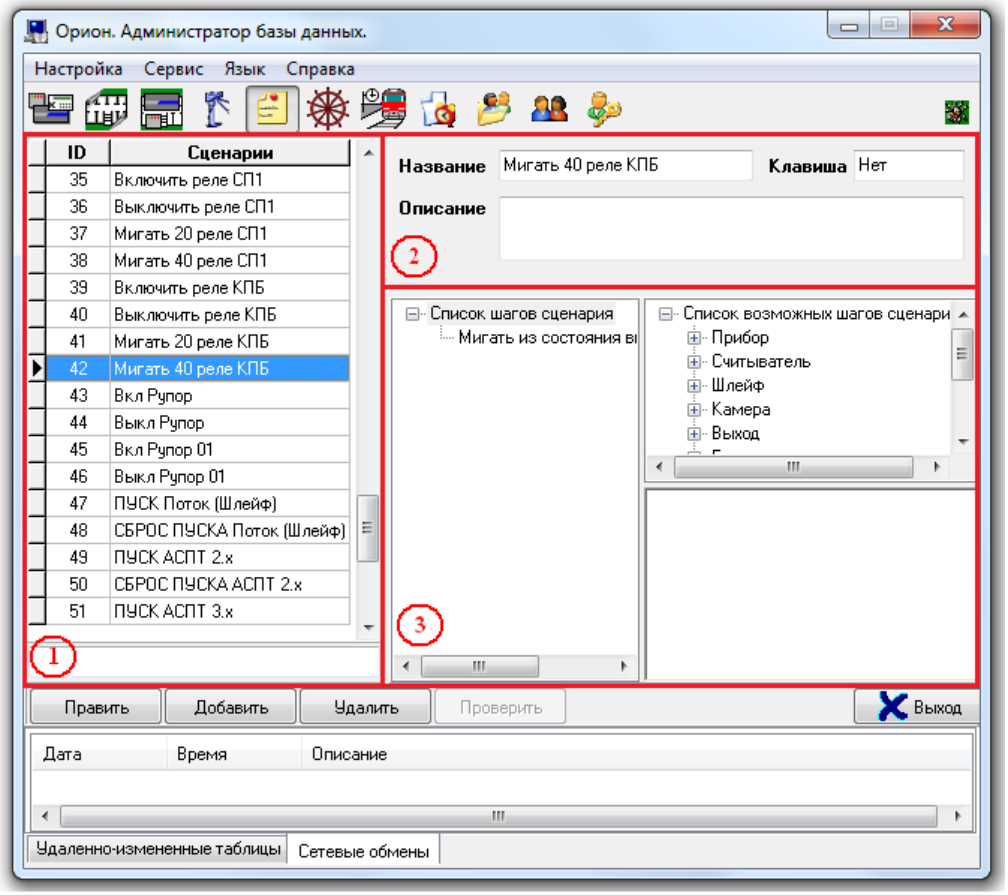

Рисунок 26 – Интерфейс модуля Администратор базы данных «Орион Про». Раздел «Сценарии управления»; 1 – список сценариев управления; 2 – свойства выбранного сценария управления; 3 – область отображения последовательности действий (шагов сценария) или текста выбранного в данный момент сценария управления, в зависимости от того, на основе шаблонов создаётся сценарий, или на основе макроязыка сценариев

В разделе «Уровни доступа» конфигурируется, в какой временной промежуток в какую зону доступа (через какую точку доступа) сотруднику может быть предоставлен доступ:

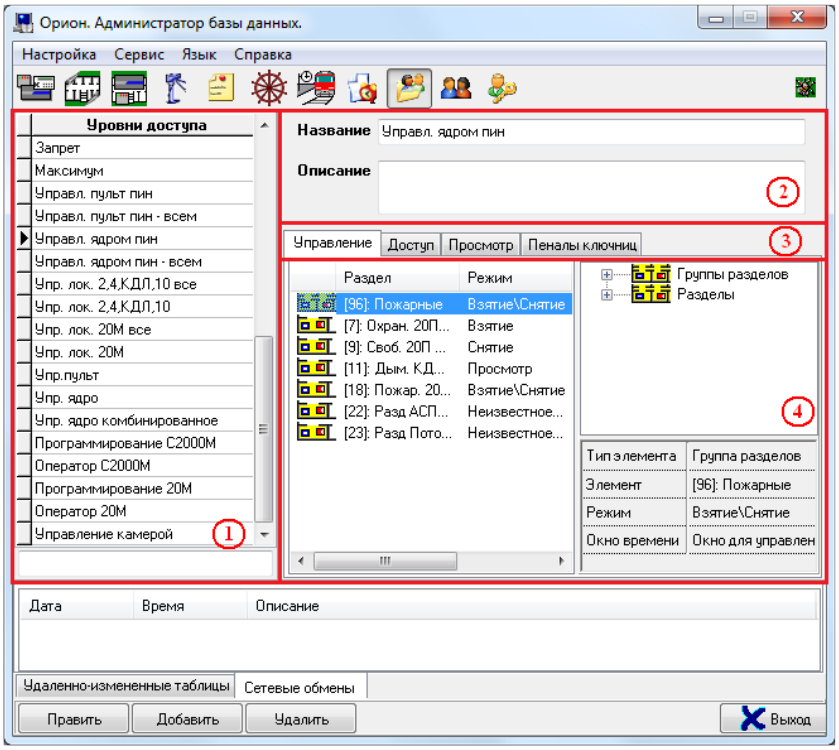

Рисунок 27 – Интерфейс модуля Администратор базы данных «Орион Про». Раздел «Уровни доступа»; 1 – список уровней доступа; 2 – свойства выбранного уровня доступа; 3 – кнопки для переключения между вкладками; 4 – область отображения выбранной вкладки текущего уровня доступа

В разделе «Сотрудники» создаются и заполняются списки компаний, подразделений, должностей, сотрудников и по каждому сотруднику принадлежность к отделу, код его личной карты доступа и т.п.:

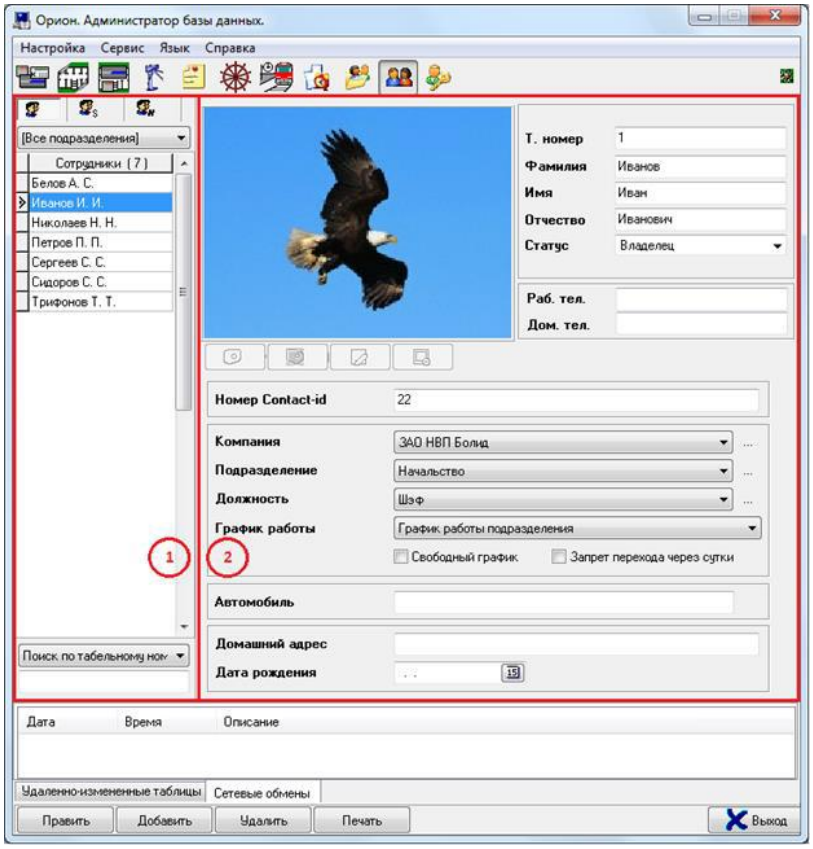

Рисунок 28 – Интерфейс модуля Администратор базы данных «Орион Про». Раздел «Сотрудники»; 1 – список сотрудников; 2 – свойства выбранного сотрудника

В разделе «Пароли» список идентификаторов базы данных сотрудников (ключей TouchMemory, Proximity–карт и отпечатков пальцев) синхронизируется с конфигураций приборов системы:

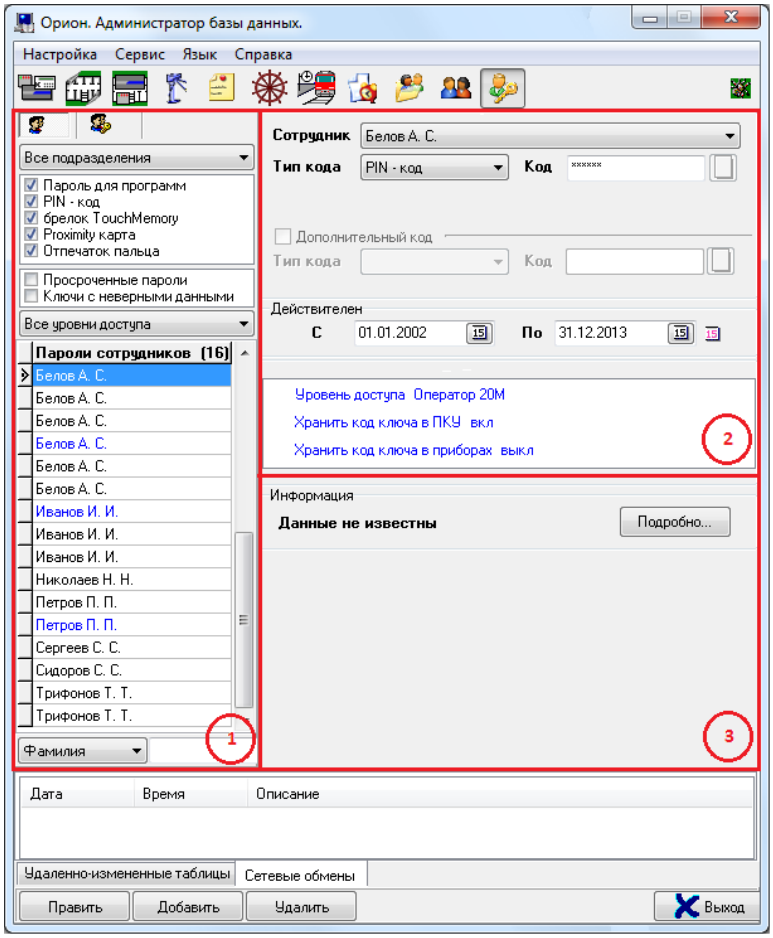

Рисунок 29 – Интерфейс модуля Администратор базы данных «Орион Про». Раздел «Пароли»; 1 – список идентификаторов; 2 – свойства выбранного идентификатора; 3 – информация о соответствии настроек базы данных для выбранного идентификатора (ключа TouchMemory, Proximity–карты или отпечатка пальца) и конфигураций приборов системы [19]

3 Выбор алгоритма и метода для проекта модернизации СКУД на предприятии Челябинское ЛПУМГ

Существующие на рынке решения систем безопасности с использованием технологий распознавания лиц, рассмотренные в главе 1 (пп. 1.9), при всех своих достоинствах и предлагаемых ими уникальных преимуществах, для внедрения на рассматриваемом предприятии достаточно затруднительны. Дело в том, что ПАО «Газпром» является критически важным предприятием нефтегазовой отрасли, одним из ключевых для экономики страны, для ее инфраструктуры. В связи с этим государство активно участвует в регулировании деятельности этой компании, что выражается в наличии множества нормативно–регулирующей документации Федерального и отраслевого уровней. Также разработаны и действуют внутренние газпромовские СТО, политики, регламенты, распоряжения и т.п. Такое положение вещей налагает существенные ограничения и вызывает определенные сложности при внедрении новых технологий и основанных на них и предлагаемых рынком решениях во всех направлениях работы дочерних компаний Газпрома. Дополнительно к вышеперечисленным можно еще привести ограничения, налагаемые законодательством в области антитеррористической деятельности и требованиями МЧС, поскольку предприятие является производственным объектом повышенной опасности и имеет категорию антитеррористической защищенности.

На сегодняшний день на рынке систем безопасности существует всего два производителя, продукты и решения которого прошли сертификацию Газпрома и являются разрешенными к внедрению на предприятиях. Это компания PERCo и НВП «Болид», чье решение, ИСО «Орион», и внедряется в настоящее время.

Поэтому в данном проекте приоритетным при выборе средств и методов модернизации СКУД является соблюдение всей регламентирующей документации и минимальные изменения в первоначальном проекте СКУД.

В ИСО «Орион» имеются все необходимые для технологии распознавания лиц аппаратные средства, а именно видеокамера с достаточными техническими характеристиками и компьютер. В свою очередь, в программном обеспечении Орион ПРО имеются возможности интеграции со сторонним программным

обеспечением. На основании вышеизложенного, было принято решение, что в рамках проекта модернизации мы будем предполагать получение необходимых для запуска распознавания лиц данных средствами внедряемой СКУД в составе ИСО «Орион». А сама технология распознавания будет основана на свободно распространяемой библиотеке алгоритмов компьютерного зрения Open Source Computer Vision Library (OpenCV), изначально разработанной и поддерживающейся компанией Intel (2000–2008 гг.), точнее, ее российским подразделением в Нижнем Новгороде. Впоследствии, благодаря полученному при разработке и поддержке библиотеки опыту, группа разработчиков перешла в американскую компанию Itseez, широко известную как разработчик программных решений в области машинного зрения [20].

3.1 Алгоритмы распознавания лиц в библиотеке OpenCV

Распознавание лиц – легкая задача для людей. Эксперименты показали, что даже дети от 1 до 3 дней от роду могут различать известные им лица [21]. Так как же трудно это сделать для компьютера? Оказывается, на сегодняшний день мы мало что знаем о распознавании лица человека. Являются ли внутренние (глаза, нос, рот) или внешние черты (форма головы, волос) наиболее важными для успешного распознавания лица? Как мы анализируем изображение и как его кодирует мозг? Дэвидом Хьюбелем и Торстеном Визелем было продемонстрировано, что наш мозг имеет специализированные нервные клетки, реагирующие на специфические локальные особенности наблюдаемой сцены, такие как линии, ребра, углы или движение. Поскольку мы не видим окружающий нас мир в виде разрозненных фрагментов, следовательно, наша зрительная кора должна каким–то образом объединять различные источники информации в значимые объекты и структуры. Автоматическое распознавание лиц заключается в извлечении этих значимых объектов из изображения, представлении их в эффективном для анализа виде и последующая их классификация.

Распознавание лиц на основе геометрических особенностей лица, вероятно, является наиболее интуитивным подходом. Одна из первых автоматизированных систем распознавания лица была описана в работе Канаде: ключевые точки (положение глаз, ушей, носа и т.д.) были использованы для построения вектора признаков (расстояние между точками, угол между ними и т.п.). Распознавание выполнялось путем вычисления евклидова расстояния между векторами признаков пробного и эталонного изображений [22]. Такой метод устойчив к изменениям освещения в силу своей природы, но имеет огромный недостаток: точная регистрация ключевых точек сложна даже при использовании современных алгоритмов. В одном из относительно недавних научных трудов по геометрическому распознаванию лиц авторства Подджио и Брунелли, был использован 22–мерный вектор признаков и эксперименты на больших наборах данных показали, что одни только геометрические признаки могут не обладать достаточной информацией для распознавания лиц [23].

Метод Eigenfaces, описанный Турком и Пентландом в своей статье, использует комплексный подход к распознаванию лица: для многомерного пространства изображения с лицом находится представление со значительно меньшим числом измерений, классифицировать которое значительно проще [24]. Маломерное подпространство находится с помощью метода главных компонент, суть которого в нахождении осей с максимальными различиями. Хотя такое преобразование является оптимальным с точки зрения реконструкции, оно не использует метки классов. Представьте ситуацию, когда различия вызваны внешними источниками, например, освещением. В этом случае оси с максимальными различиями вовсе не обязательно будут содержать информацию о реальных различиях, поэтому классификация становится невозможной. Таким образом, в теме распознавания лиц появился метод класс–ориентированной проекции изображения с использованием анализа линейного дискриминанта, представленный Белхьюмером, Гиспанной и Кригманом. Основная идея состоит в том, чтобы минимизировать различия внутри одного класса, одновременно увеличивая различия между классами [25].

В последнее время появились различные методы для выделения локальных признаков. Речь о том, чтобы избежать высокой размерности входных данных, описываются только локальные области изображения и – очень хочется надеется на это – извлеченные таким образом признаки более устойчивы к частичному перекрытию, освещению и небольшому размеру изображения. Алгоритмами для выделения локальных признаков являются Вейвлеты Габора (см. [26]), дискретное преобразование косинуса (см. [27]) и локальные двоичные шаблоны (см. [28]). По–прежнему остается открытым вопрос о том, какой метод лучше всего позволяет сохранить пространственную информацию при выделения локальных признаков, поскольку эта информация является потенциально полезной.

3.1.1 Алгоритм Eigenfaces

Главная проблема, которая возникнет при представлении изображения для нужд работы алгоритма – это его высокая размерность. Двумерные изображения в оттенках серого охватывают a–мерное векторное пространство, поэтому изображение с пикселями уже находится в a–мерном пространстве изображения. Вопрос в том, являются ли все измерения одинаково полезными для нас? Мы можем принять решение только при условии, если есть какая–либо разница в данных, поэтому мы ищем компоненты, на которые приходится большая часть информации. Метод главных компонент позволяет превратить множество возможно подобных переменных в меньший набор различных. Идея состоит в том, что высокоразмерный набор данных часто описывается идентичными переменными, при этом действительно значимых измерений значительно меньше по сравнению со всем объемом данных. Метод PCA находит направления с наибольшими различиями в данных, называемые главными компонентами.

Итак, данный алгоритм предполагает, что все изображения имеют одинаковые размерности по ширине и высоте, представлены в оттенках серого и центрированы, т.е. глаза, нос, губы должны находиться на приблизительно одном уровне.

На этапе обучения создается обучающая выборка, строится ковариационная матрица, вычисляются собственные вектора и значения, определяются их веса.

1. Создание матрицы обучающих векторов

Получаемое на вход изображение в обобщенном виде представляет собой матрицу $r \times c$. Это изображение преобразуется в один вектор путём конкатенации строк.

$$I = \begin{bmatrix} d_{0,0} & d_{0,1} \dots & d_{0,c} \\ d_{1,0} & d_{1,1} & \\ \vdots & & \\ d_{r,0} & & d_{r,c} \end{bmatrix} \rightarrow V = \begin{bmatrix} d_{0,0} \\ d_{0,1} \\ \vdots \\ d_{0,c} \\ d_{1,0} \\ \vdots \\ d_{r,c} \end{bmatrix}, \quad (1)$$

где I – матрица исходного изображения,

$d_{i,j}$– интенсивность оттенка серого в конкретном пикселе,

r – размер изображения в высоту в пикселях,

c – размер изображения в ширину в пикселях,

$V-$ результирующий вектор изображения.

Все изображения преобразовываются в вектора и образуют матрицу обучающей выборки $W = \{V_0, V_1, \dots, V_n\}$, где n – количество изображений в обучающей выборке.

2. Нормирование обучающей матрицы

На данном шаге рассчитывается среднее изображение *M:*

$$M = \frac{1}{n}\sum_{i=1}^{n} V_j \ . \quad (2)$$

После чего создается новый набор векторов, каждый из которых представляет собой один из первоначальных изображений за вычетом среднего:

$$\Phi = (\Phi_1, \Phi_2, \dots, \Phi_n).$$

$$\Phi_i = V_i - \mathrm{M}, \mathrm{i} = 1, \dots, \mathrm{n}. \quad (3)$$

Этот шаг необходим для того, чтобы каждый вектор нес только уникальную информацию об изображении

3. Построение ковариационной матрицы и получение собственных векторов и значений

Ковариационная матрица, получаемая по [формуле 4] имеет размерность $L^2 \times L^2$, где $L = r \cdot c$, что предполагает в дальнейшем расчет L^2 собственных векторов и значений:

$$\mathrm{C} = \frac{1}{n}\sum_{i=1}^{n} \Phi_i \Phi_i^T = AA^T, \quad (4)$$

где $A = [\Phi_1, \Phi_2, \dots, \Phi_n]$.

Для уменьшения количества обрабатываемых данных рассчитывается меньшая ковариационная матрица $\tilde{C} = A^T A$, размерность которой равна $n \times n$. Соотношение собственных векторов λ и значений u матрицы C и собственных векторов $\tilde{\lambda}$ и значений $\tilde{u}$ матрицы $\tilde{C}$ продемонстрировано на формуле:

$$\lambda_i = \bar{\lambda_i};\ u_i = \bar{\lambda_i}^{-1/2} i A \bar{u_i} \quad (5)$$

4. Расчет весов собственных значений

На данном шаге рассчитывается матрица весов, с какими каждый собственный вектор влияет на матрицу.

$$\Omega = \lambda^T A, \quad (6)$$

где Ω – матрица весов, размерностью $n \times n$,

$\lambda = [\lambda_1, \lambda_2, \dots, \lambda_n]$– матрица собственных векторов ковариационной матрицы.

На этапе распознавания используются матрицы весов Ω и собственных векторов λ, полученные в ходе обучения, для проецирования нового изображения в новое пространство.

1. Преобразование входного тестового изображения в новое пространство собственных векторов.

Тестовое изображение преобразуется в вектор аналогично обучающим по [формуле 1] и нормируется по среднему [формула 3]. После чего производится преобразование:

$$w = \lambda^T x, \quad (7)$$

где w– вектор преобразованного тестового изображения,

x – вектор входного изображения.

2. Кластеризация и поиск расстояний

После перехода в новое пространство необходимо определить, к какому из обучающих векторов ближе всего находится распознаваемое изображение. Для решения этой задачи могут использоваться две метрики: евклидово расстояние и расстояние Махаланобиса.

А) Евклидово расстояние.

Расстояние d по Евклиду между двумя векторами a и b рассчитывается

следующим образом:

$$d = \sqrt{a^T b}. \quad (8)$$

Б) Расстояние по Махаланобису.

Расстояние по Махаланобису помимо самих векторов учитывает и ковариационную матрицу *C*. Рассчитывается по формуле:

$$d = \sqrt{(a-b)^T C^{-1}(a-b)}, \quad (9)$$

где C^{-1} – инвертированная ковариационная матрица.

В контексте рассматриваемой задачи необходимо рассчитать расстояния между вектором *w* и каждым вектором матрицы весов Ω:

$$d_j = dist(w, \Omega_j), i = 1,2, \dots n, \quad (10)$$

где d_j – расстояние по Евклиду между тестовым изображением и j–тым изображением обучающей выборки,

dist(a, b) – функция, рассчитывающая евклидово расстояние между векторами a и b,

Ω_j – j–тый вектор матрицы весов Ω.

Альтернативно рассчитывается расстояние по Махаланобису:

$$d_j = dist(w, \mathrm{C}, \Omega_j), i = 1,2, \dots n, \quad (11)$$

где d_j – расстояние Махаланобиса между тестовым изображением и j–тым изображением обучающей выборки,

$dist(a, \mathrm{C}, b)$– функция расчета расстояния Махаланобиса между векторами a и b по ковариационной матрице *C*.

Таким образом формируется вектор расстояний $d = (d_1, d_2, \dots, d_n)$.

3. Поиск вектора с наибольшим сходством и установка критерия отсечения изображений

   В полученном векторе расстоянии d находится минимальное значение и его индекс:

$$R_0 = \min(d),$$
$$R_1 = ind(R_0, d), \quad (12)$$

где $R = (x, y)$ – вектор из двух элементов, хранящий минимально расстояние и его

индекс в векторе расстояний,

min(a) – функция поиска минимально значения в векторе,

ind(x, a) – функция поиска индекса элемента x в векторе a.

В результате данных операций находится минимальное расстояние и индекс соответствующего изображения обучающей выборки. Однако он рассчитывается и для изображений, которые не принадлежат обучающей выборке, для отсечения таковых вводится эмпирический критерий *O*, расстояния большие которого идентифицируются как не принадлежащие выборке.

3.1.2 Алгоритм Fisherfaces

Данный алгоритм является расширением алгоритма Eigenface. Отличием является кластеризация обучающих векторов, для чего рассчитываются внутри–классовые и между–классовые ковариационные матрицы.

$$S_b = \sum_{i=1}^{c} \sum_{x \in X_i} (x - m_i)(x - m_i)^T, \quad (13)$$

где c – количество классов в выборке

x–вектор, принадлежащий классу X_i,

m_i–средний вектор i–го класса.

$$S_b = \sum_{i=1}^{c} N_i (m_i - m)(m_i - m)^T, \quad (14)$$

где c – количество классов,

N_i– количество элементов в i–том классе,

m_i– средний вектор i–го класса,

m– средний вектор всей выборки.

Следующим шагом рассчитывается матрица главных компонент:

$$W_{PCA} = \arg max_W W^T S_T W, \quad (15)$$

где W – вектор тестового изображения,

S_T – ковариационная матрица.

Завершающим шагом является расчет итоговой матрицы:

$$W_{PCA} = \arg max_W \frac{|W^T W_{PCA}^T S_b W_{PCA} W|}{|W^T W_{PCA}^T S_w W_{PCA} W|}. \quad (16)$$

3.1.3 Алгоритм локальных двоичных шаблонов (LBPH)

Главная идея алгоритма в том, чтобы извлекать признаки из окрестностей изображения, этот набор признаков имеет маломерную структуру, что является положительной чертой данного метода. Также, поскольку признаки извлекаются из окрестностей, это позволяет быть алгоритму устойчивым к масштабу, поворотам и т.д.

Описание работы метода LBPH: сначала изображение делится на одинаковые блоки, которые образуют сетку (см. Рисунок 30).

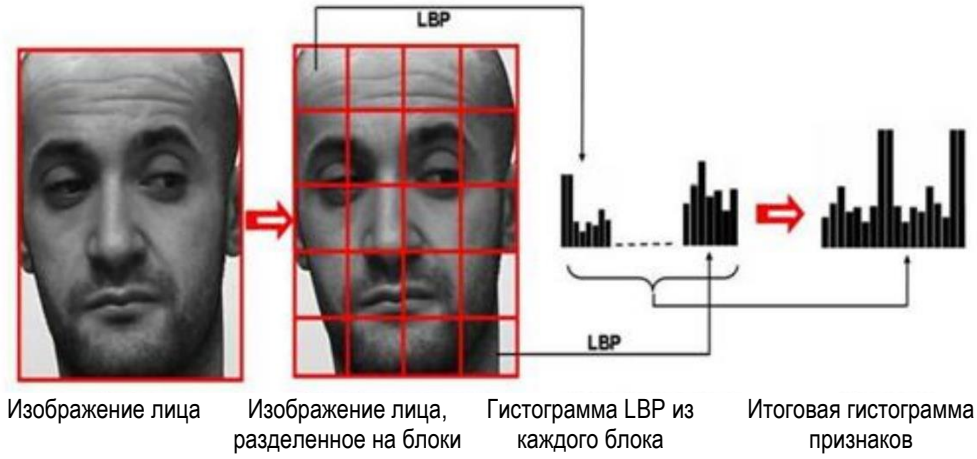

Рисунок 30 – Схема работы алгоритма LBPH

Далее для каждого блока строится гистограмма кодов, которые вычисляются таким образом: берется пиксель, который сравнивается с соседями, если интенсивность центрального пикселя больше или равна интенсивности соседа, то он обозначается 1, иначе — 0. В итоге каждому пикселю будет соответствовать двоичное число, состоящее из результатов сравнений. Эти преобразования наглядно показаны на Рисунок 31. Полученные гистограммы объединяются в одну общую, которая является итоговым дескриптором, который используется для классификации лица.

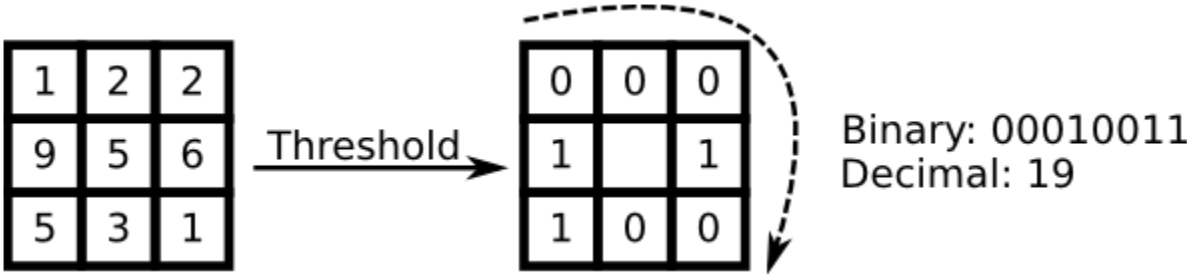

Рисунок 31 – Преобразование области в двоичный код

Описанный подход позволяет захватывать очень мелкозернистые детали, позже оказалось, что LBPH не мог кодировать детали разного масштаба, из–за этого он был расширен, и теперь число соседей может варьироваться. Идея расширения заключалась в том, чтобы расположить соседей по кругу определенного радиуса, и, таким образом, выделялись следующие признаки окрестностей (см. Рисунок 32).

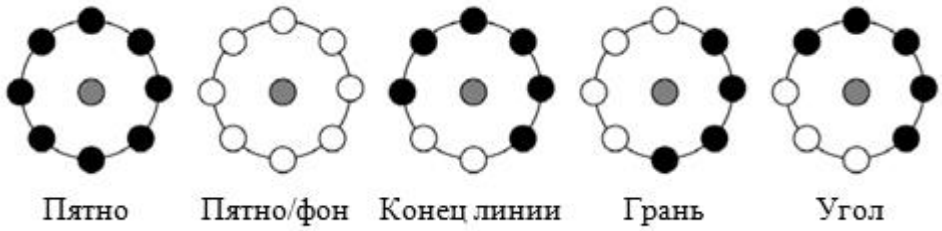

Рисунок 32 – Признаки круговой окрестности

Формулы для расчета координат соседей:

$$x_p = x_c + R\cos\left(\frac{2\pi p}{P}\right)$$

$$y_p = y_c + R\sin\left(\frac{2\pi p}{P}\right), \quad (17)$$

где x_p, y_p – координаты соседа;

x_c, y_c – координаты центра;

R – радиус окружности;

p – номер соседа;

P – количество соседей.

Если координаты точек не соответствуют координатам изображения, к ним будет применен метод интерполяции.

Итак, мы рассмотрели несколько наиболее известных алгоритмов

распознавания лиц, предлагаемых библиотекой OpenCV. Теперь необходимо выбрать оптимальный для нашего проекта.

Алгоритмы Eigenfaces and Fisherfaces применяют целостный подход к распознаванию лиц. Мы имеем дело с данными в виде векторов где–то в многоразмерном пространстве изображения. Высокую размерность при этом мы преобразуем в низкоразмерное подпространство, где очень надеемся, что останется какая–то полезная информация. Как уже было замечено ранее, подход Eigenfaces максимизирует общий разброс, что может привести к проблемам, если различия генерируются внешним источником, поскольку компоненты с максимальными различиями по всем классам часто усложняют классификацию. Таким образом, качество этих алгоритмов сильно зависит от входных данных.

В реальной жизни, конечно же, никому не нужны алгоритмы, требующие близкие к идеальным входные данные. Невозможно гарантировать ни идеальные настройки освещения в изображениях, ни 10 разных изображений одного человека. Может быть так, что для каждого человека будет только один образ. Оценки ковариации для подпространства могут быть совершенно неправильными, таким же будет и результат распознавания. Опытным путем было проверено, что метод Eigenfaces имел коэффициент распознавания 96% даже на идеальной учебной базе данных лиц AT & T Facedatabase с 10 вариантами фото для каждого человека.

Поэтому в своем проекте я отдам предпочтение алгоритму LBPH, менее требовательному ко входным данным.

3.2 Методика взаимодействия со СКУД

Как было показано во второй главе (пп. 2.3.2), инструментарий сценариев модуля «Администратор БД» программного комплекса «Орион Про» специально предназначен для выполнения нетиповых задач и дает возможность «тонкой настройки» системы и внесения в неё дополнительной функциональности.

Средствами сценария есть возможность запустить определенную последовательность действий при возникновении события прохода сотрудника, а именно, при прикладывании карты к считывателю запустить фотосъемку проходящего с последующим сохранением серии фотографий во внешний каталог, а также получить и сохранить там же фото сотрудника из базы данных для сверки с полученными фотографиями.

Блок-схема алгоритма действий по подготовке входной информации для модуля распознавания лиц программными и аппаратными средствами СКУД представлена на Рисунок 33, блок-схема сценария – на Рисунок 34.

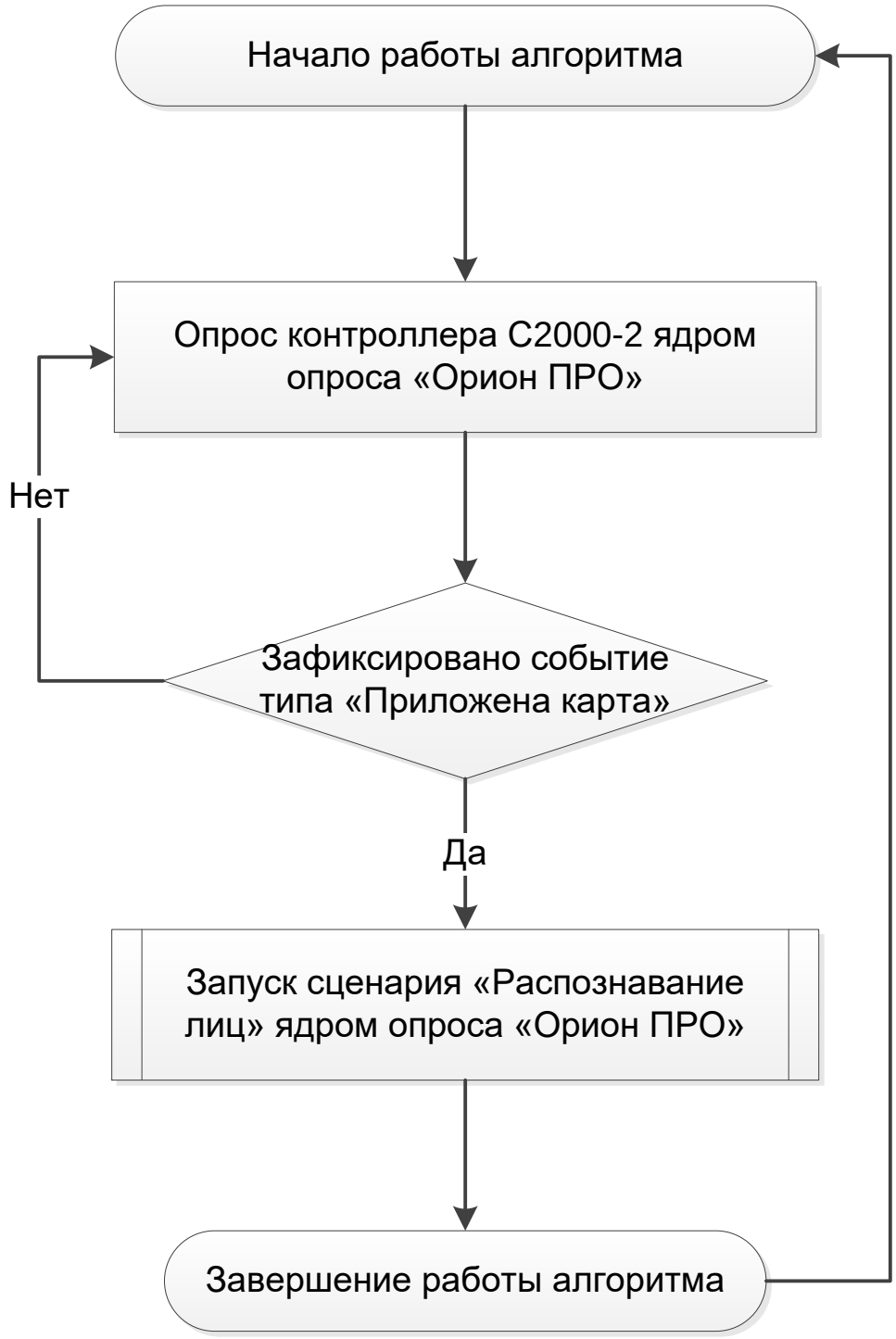

Рисунок 33 – Блок-схема алгоритма действий по подготовке входной информации для модуля распознавания лиц

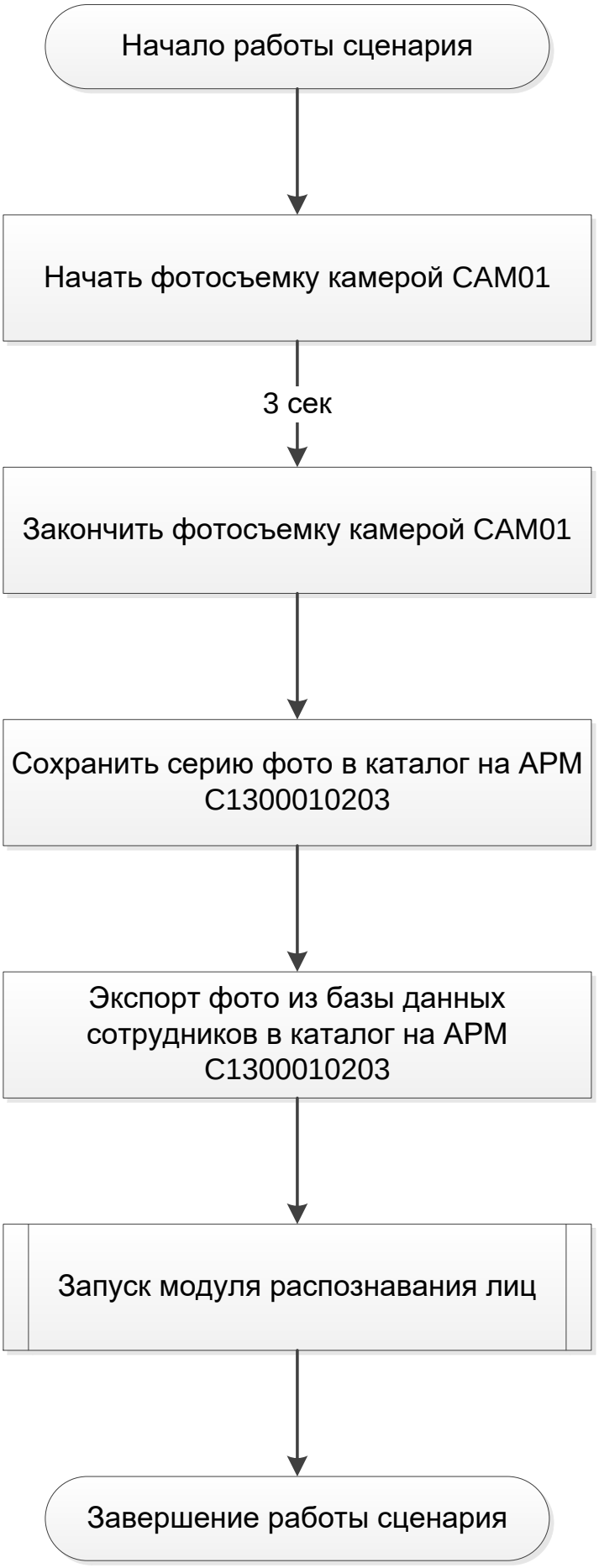

Рисунок 34 – Блок-схема сценария «Распознавание лиц»

4 Программное обеспечение проекта модернизации СКУД на основе ИСО «Орион» с использованием выбранного алгоритма распознавания лиц из библиотеки OpenCV

4.1 Подготовка сценария средствами ПО «Орион ПРО»

Прежде чем начать создание сценария, необходимо включить свойство «Обработка событий» для объекта «Турникет» на странице «Доступ». Выбираем объект системы (турникет), по событиям от которого будет запускаться сценарий. В появившемся окне справа находим внизу строку «Обработка событий» и из раскрывающегося списка выбираем тип события «Приложена карта»:

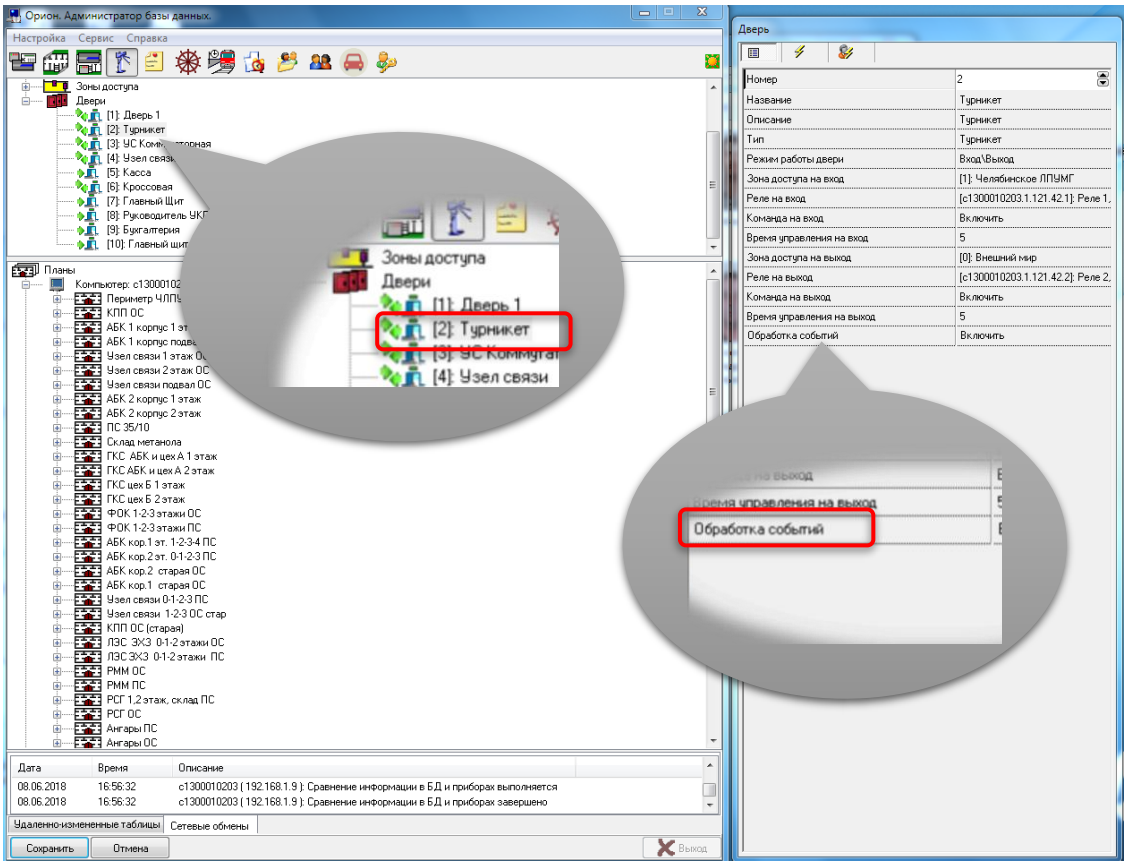

Рисунок 35 – Создание сценария. Шаг 1

Подготовка сценариев управления ведется на странице «Сценарии управления». После выбора типа события мы автоматически попадаем на страницу «Сценарии управления», где начинаем создавать сценарий.

Первым шагом будет «Начать запись», т.е. при прикладывании сотрудником карты включается фотосъемка – параметры задаются в правой нижней зоне окна:

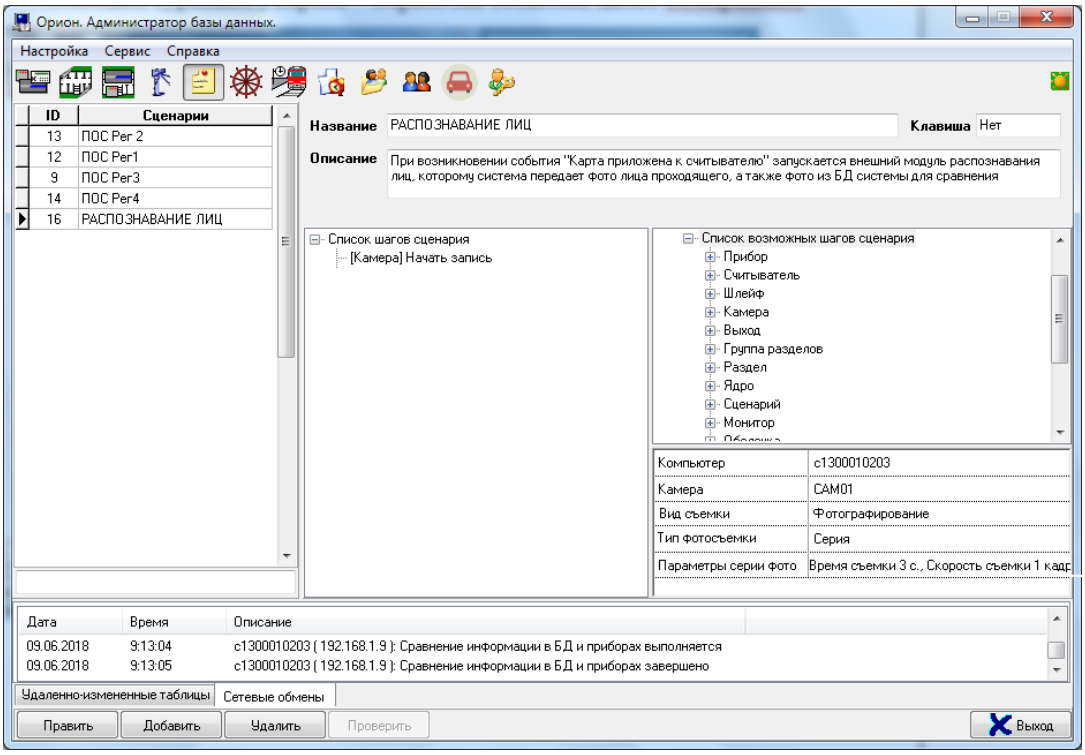

Рисунок 36 – Создание сценария. Шаг 2

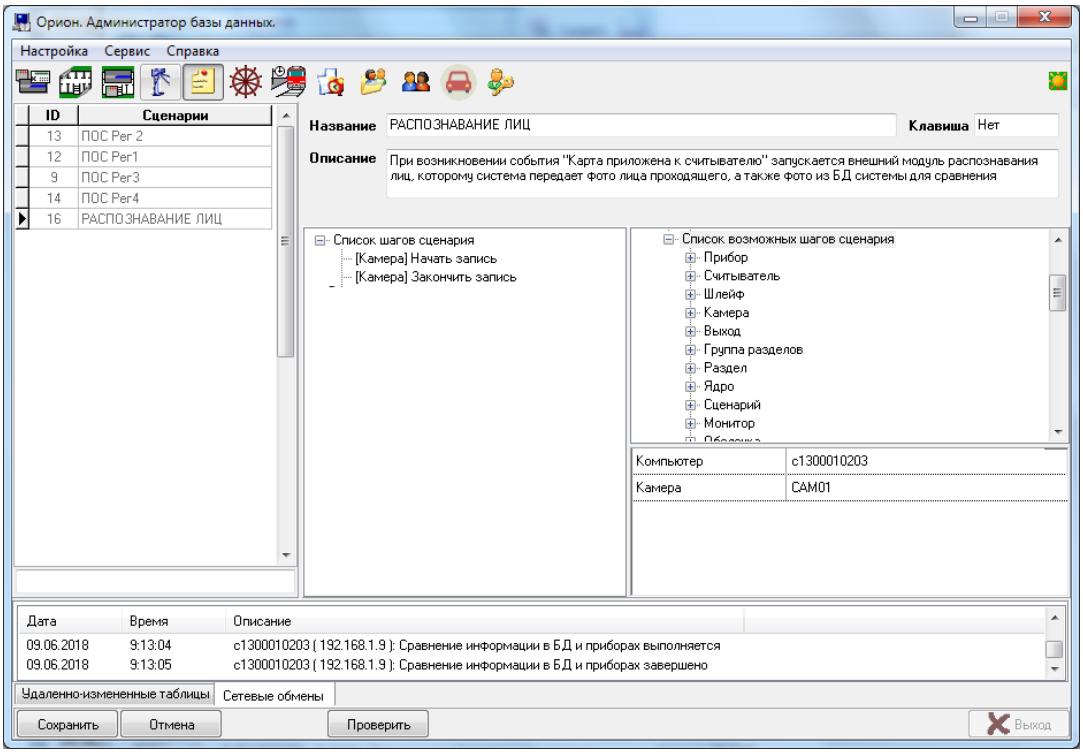

Рисунок 37 – Создание сценария. Шаг 3

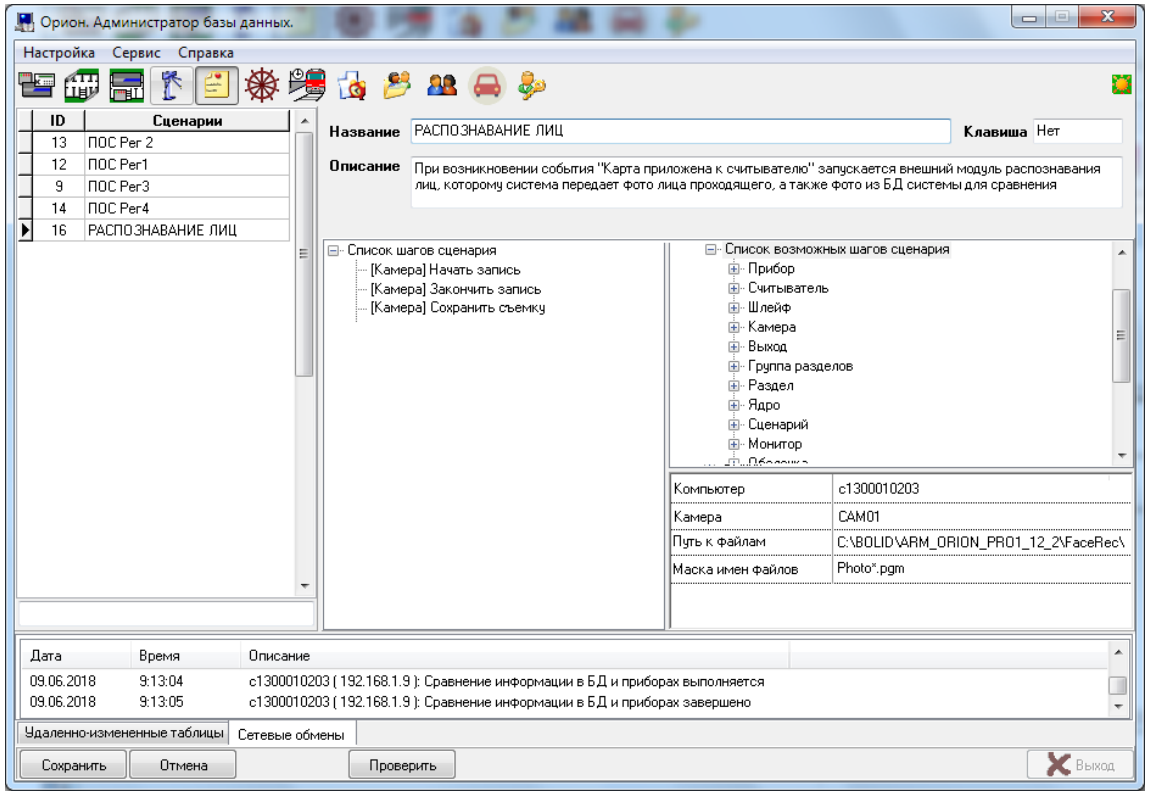

Рисунок 38 – Создание сценария. Шаг 4

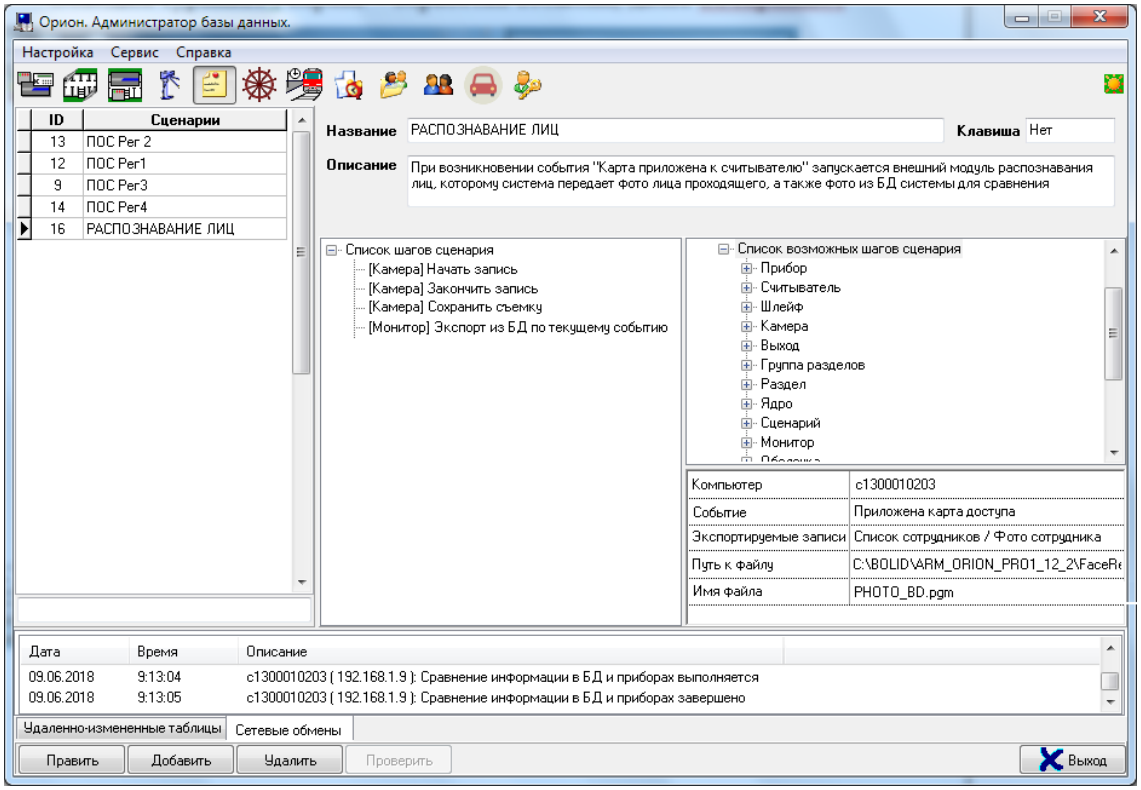

Рисунок 39 – Создание сценария. Шаг 5

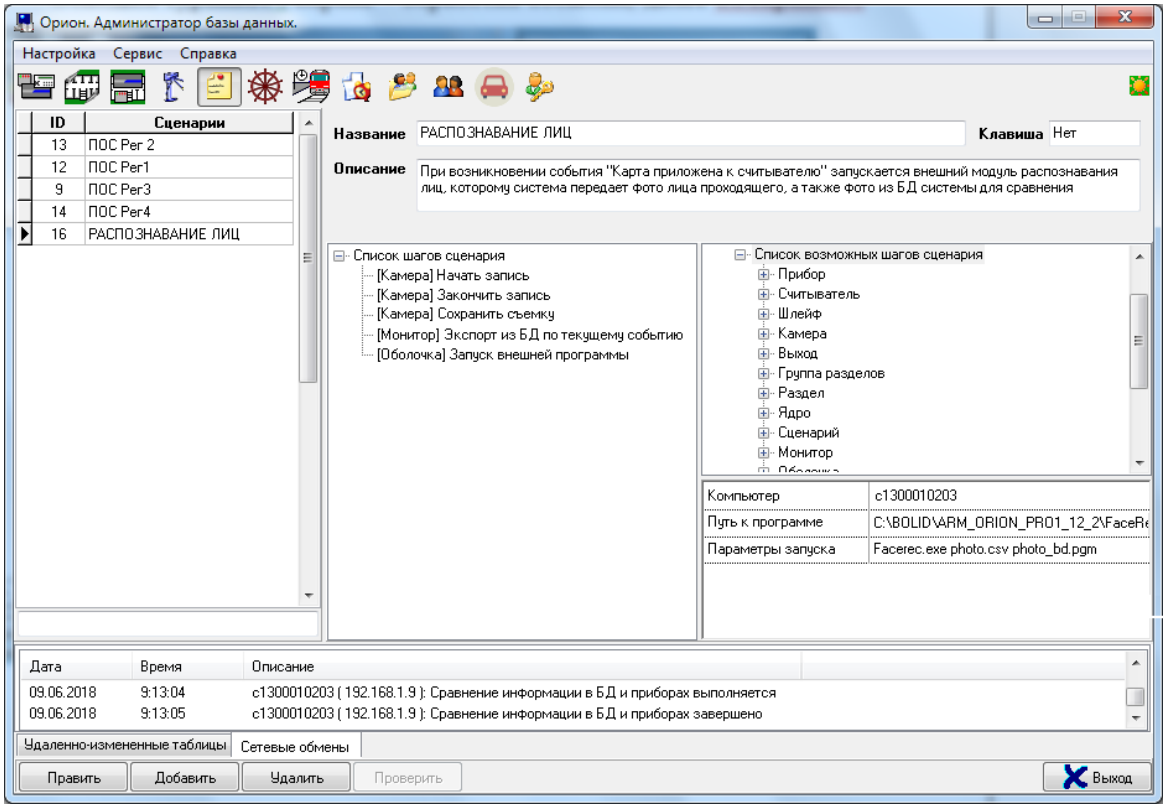

Рисунок 40 – Создание сценария. Шаг 6

4.2 Разработка программного модуля распознавания лиц в среде разработки Visual Studio

Для разработки программного модуля была использована Microsoft Visual Studio — линейка продуктов компании Microsoft, включающих интегрированную среду разработки программного обеспечения и ряд других инструментальных средств. Данные продукты позволяют разрабатывать как консольные приложения, так и приложения с графическим интерфейсом, в том числе с поддержкой технологии Windows Forms, а также веб–сайты, веб–приложения, веб–службы как в родном, так и в управляемом кодах для всех платформ, поддерживаемых Windows, Windows Mobile, Windows CE, .NET Framework, Xbox, Windows Phone .NET Compact Framework и Silverlight.

Visual Studio включает в себя редактор исходного кода с поддержкой технологии IntelliSense и возможностью простейшего рефакторинга кода. Встроенный отладчик может работать как отладчик уровня исходного кода, так и отладчик машинного уровня. Остальные встраиваемые инструменты включают в себя редактор форм для упрощения создания графического интерфейса приложения, веб–редактор, дизайнер классов и дизайнер схемы базы данных. Visual Studio позволяет создавать и подключать сторонние дополнения (плагины) для расширения функциональности практически на каждом уровне, включая добавление поддержки систем контроля версий исходного кода (как, например, Subversion и Visual SourceSafe), добавление новых наборов инструментов (например, для редактирования и визуального проектирования кода на предметно–ориентированных языках программирования) или инструментов для прочих аспектов процесса разработки программного обеспечения (например, клиент Team Explorer для работы с Team Foundation Server).

Листинг программного модуля представлен в Приложении А.

По результатам работы алгоритма выводится сообщение о том, соответствует ли проходящий сотрудник данным в базе на основании приложенной им карты доступа или нет (нарушитель).

ЗАКЛЮЧЕНИЕ

В первой главе были даны основные понятия об объекте управления – СКУД на современном промышленном предприятии: принципы ее проектирования, предъявляемые при постановке задачи требования, классификация и состав СКУД. Был проведен обзор существующих решений СКУД. С целью проведения исследования осуществлён обзор существующих решений СКУД с использованием технологий распознавания лиц. Проведённое исследование показало, что на рынке предлагается достаточное количество решений «под ключ», но всех их объединяет одно – отсутствие сертификации Газпром. Поэтому было принято решение модернизировать внедряемую СКУД «Орион», соответствующую всем регламентирующим документам.

Во второй главе подробно был описан существующий уровень автоматизации, а именно внедряемая на предприятии СКУД на основе ИСО «Орион», реализуемый в ее рамках функционал, состав оборудования и программное обеспечение «Орион Про».

В третьей главе в качестве методического обеспечения проекта модернизации была выбрана встроенная в программное обеспечение «Орион» функциональная возможность интеграции с внешним программным обеспечением. Были раскрыты ключевые понятия алгоритмов распознавания лица и был сделан обзор трех из доступных в библиотеке OpenCV алгоритмов распознавания, в итоге был выбран один наиболее соответствующий нашим требованиям – алгоритм LBPH.

В четвертой главе в качестве программного обеспечения проекта была представлена разработка программного модуля в среде разработки Microsoft Visual Studio 2017, а также конфигурирование ПО «Орион» на работу с этим модулем.

Представленный проект модернизации является лишь частным примером применения одной из технологий машинного зрения. В дальнейшем предполагается реализовать другие подобные решения, например, автоматический анализ и выявление посторонних предметов и подозрительных вещей на проходной, система уведомления охраны о наличии у проходящего необходимых к досмотру предметов в руках и т.п.

Данный проект был принят в качестве изменений к основному проекту внедрения СКУД и согласован в отделе инженерно-технических средств охраны Службы корпоративной защиты ООО «Газпром Трансгаз Екатеринбург». Его ввод в эксплуатацию запланирован на IV квартал 2018 года.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Волхонский, В.В. Системы контроля и управления доступом. Учебное пособие / В.В.Волхонский. – СПб: Университет ИТМО, 2015. – 105 с.

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

3 Проектирование СКУД: эксперты советуют / А.Е. Гамбург, Е.Н. Ильина, А.М. Омельянчук, С.В. Соловьев, А.Ю. Сизов, Н.В. Кукушин, Е.А. Синченко, А.В. Катренко, А.С. Большаков // Системы безопасности. – http://www.secuteck.ru/articles2/sys_ogr_dost/proektirovanie–skyd–eksperti–sovetyut/.

4 ГОСТ Р 51241–98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. – М.: Изд–во стандартов, 2000. – 34 с.

5 ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – М.: Изд–во стандартов, 2008. – 7 с.

6 ГОСТ Р 52435–15. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний. – М.: Стандартинформ, 2016. – 28 с.

7 Рекомендации РД 78.36.002–2010. Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения. – М.: Стандартинформ, 2010. – 13 с.

8 Контроль и управление доступом // Безопасность, управление и автоматизация: статьи, обзоры, аналитика, советы. – https://video–praktik.ru/skud.html.

9 Обзор решений: СКУД и УРВ на предприятии. Проходная: турникет, шлагбаум, двери // Techportal.ru – http://www.techportal.ru/review/skud_i_urv/#first.

10 СКУД SIGUR // Документация по системе и ее аппаратным компонентам. Официальный сайт компании ПромАвтоматика. – http://www.sigursys.com.

11 СКУД PARSECNet3 // Документация по системе и ее аппаратным компонентам. Официальный сайт компании ООО «НПО Релвест». –

https://www.parsec.ru/security-system.

12 СКУД Smartec // Документация по системе и ее аппаратным компонентам. Официальный сайт компании «СМАРТЕК СЕКЬЮРИТИ». – http://www.smartec-security.com.

13 Стоянов, Ю.М. Особенности внедрения и использования систем контроля доступа по лицу / Ю.М. Стоянов // Системы безопасности. – http://www.secuteck.ru/articles2/sys_ogr_dost/osobennosti-vnedreniya-i-ispolzovaniya-sistem-kontrolya-dostupa-po-litsu.

14 Масштабируемая и функциональная СКУД «СтилПост» от компании «Стилсофт» // Системы безопасности. – http://www.secuteck.ru/articles2/sys_ogr_dost/masshtabiruemaya-i-funktsionalnaya-skud-stilpost-ot-kompanii-stilsoft.

15 «Каскад-Контроль» – интегрированная СКУД на базе биометрической системы идентификации личности. 80 новинок весны представляют участники ТБ-Форума 2012 // Системы безопасности. – http://www.secuteck.ru/articles2/test/80-novinok-vesni.

16 Автоматизированная система контроля доступа «Каскад-контроль». Краткое описание возможностей системы // Официальный сайт группы компаний «Техносерв». – http://www.technoserv.com/img/kaskad/kaskad_kontrol.pdf.

17 Ершаков, К.С. Продвинутые технологии распознавания. Развитие 3D-идентификации и сканирования лица / К.С. Ершаков // Системы безопасности. – http://www.secuteck.ru/articles2/sys_ogr_dost/prodvinutye-tehnologii-raspoznavaniya-razvitie-3d-identifikatsii-i-skanirovaniya-litsa.

18 Интегрированная система охраны «Орион» // Документация по системе и ее аппаратным компонентам. Официальный сайт НВП «Болид».– http://www.bolid.ru/production/orion.

19 АРМ «Орион Про», версия 1.12. Руководство по эксплуатации // Официальный сайт НВП «Болид».– http://www.bolid.ru/production/orion/po–orion.

20 Корняков, К.С. Краткая история проекта OpenCV. Блог компании Itseez / К.С. Корняков // «Хабр» – https://habr.com/company/intel/blog/146434.

21 Turati, C. Newborns face recognition: Role of inner and outer facial features /

Turati C., Macchi Cassia V., Simion F., Leo I. // Child Development 77, 2 (2006), p.297–311.

22 Kanade, T. Picture processing system by computer complex and recognition of human faces / T. Kanade // PhD thesis, Kyoto University, November 1973.

23 Brunelli, R. Face Recognition through Geometrical Features / R.Brunelli, T.Poggio // European Conference on Computer Vision (ECCV). Compilation, 1992, p. 792–800.

24 Turk, M. Eigenfaces for recognition / M. Turk, A. Pentland // Journal of Cognitive Neuroscience 3 (1991), p.71–86.

25 Belhumeur, P. N. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection / P.N. Belhumeur, J. Hespanha, D. Kriegman // IEEE Transactions on Pattern Analysis and Machine Intelligence 19, 7 (1997), p.711–720.

26 Wiskott, L. Face Recognition By Elastic Bunch Graph Matching. / L.Wiskott, J.Fellous, N.Krüger, C.Malsburg // IEEE Transactions on Pattern Analysis and Machine Intelligence 19 (1997), p. 775–779.

27 Messer, K. Performance Characterization of Face Recognition Algorithms and Their Sensitivity to Severe Illumination Changes / K. Messer. In: ICB, 2006, p.1–11.

28 Ahonen, T. Face Recognition with Local Binary Patterns / T. Ahonen, A. Hadid, M. Pietikainen // European Conference on Computer Vision (ECCV). Compilation, 2004, p.469–481.

29 Wang, L., Zhang J., Zang F. An Efficient Feature Extraction Method, Global Between Maximum and Local WithinMinimum, and Its Applications. Mathematical Problems in Engineering, 2011, july. doi:10.1155/2011/176058.

30 Система контроля и управления доступом // Википедия. – https://ru.wikipedia.org/wiki/Система_контроля_и_управления_доступом.

31 Архив выпусков журнала // Грани безопасности. – https://www.tinko.ru/journal.

32 Распознавание лиц на групповых фотографиях с использованием алгоритмов сегментации / А.И. Шерстобитов, В.П. Федосов, В.А. Приходченко, М.В. Тимофеев // Известия Южного федерального университета. Технические науки. – 2013. – С. 66–72.

33 Применение скрытых марковских моделей с одномерной топологией к задаче распознавания лиц / Т.А. Гультяева // Материалы российской научно-технической конференции «Информатика и проблема телекоммуникаций», 2006. – Новосибирск: СибГУТИ. Том I, с. 150-154.

34 Рыкунов, В.Д. Охранные системы и технические средства физической защиты объектов / В.Д. Рыкунов. – М.: Секьюрити Фокус, 2011. – 288 с.

35 Синилов, В.Г. Системы охранной, пожарной и охранно-пожарной сигнализации / В.Г. Синилов. – М.: Издательский центр «Академия», 2010. – 509 с.

36 Применение скрытых марковских моделей с одномерной топологией к задаче распознавания лиц / Т.А. Гультяева // Материалы российской научно-технической конференции «Информатика и проблема телекоммуникаций», 2006. – Новосибирск: СибГУТИ. Том I, с. 150-154.

37 Кудряшов, П.П. Алгоритмы обнаружения лица человека для решения прикладных задач анализа и обработки изображений: автореф.дис. Кудряшова П.П., кандидата технических наук / П.П. Кудряшов. – Волгоград: Изд-во ВГТУ, 2007. – 107 с.

38 Поршенинников, К.П. Событийно-ориентированные системы контроля доступа в условиях промышленности / К.П. Поршенинников. – Н. Новгород.: Интеко-Пресс, 2011. – 213 с.

39 Кушелев, П.А. Технические аспекты проектирования систем безопасности / П.А. Кушелев. – Уфа: Алфавит, 2013. – 113 с.

40 Астраханцева, Л.А. Роль систем контроля доступа в антитеррористической защищенности объектов ТЭК / Л.А. Астраханцева. – М.: Секьюрити Фокус, 2009. – 325 с.

41 Кориолисов, Е.А. Обзор оборудования для видеонаблюдения и доступа / Е.А. Кориолисов. – СПб: Ленкнига, 2015. – 372 с.

42 Рвезенцев, И.В. Программируемые контроллеры систем доступа / И.В. Рвезенцев; под ред. проф. В.П. Мудкирского. – М.: СОЛОН-Пресс. – 2015. – 208 с.

43 Дочурский, Н.П. Объектно-ориентированные среды разработки как инструмент конфигурирования систем безопасности. / Н.П. Дочурский. – М.: Изд-во МГТУ им. Н.Э. Баумана. – 2009. – 362 с.

44 Лазарев, Ю. Моделирование процессов и систем в Matlab. Учебный курс / Ю. Лазарев. – СПб.: Питер; Киев: Издательская группа BHV, 2005. – 512 с.

45 Харченко, А.А. Инженерно-технические средства охраны промышленных предприятий. / А.А. Харченко. – Таганрог: ТТИ ЮФУ. – 2010. – 543 с.

46 ГОСТ 21.208–2013 СПДС. Автоматизация технологических процессов. Обозначения условные приборов и средств автоматизации в схемах. – М.: Стандартинформ, 2015.

47 ГОСТ 19.701–90 (ИСО 5807–85) ЕСПД. Схемы алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения. – М.: Стандартинформ, 2010.

48 Первый рубеж охраны: мнения экспертов об особенностях охраны периметра в городской среде / Д.А. Цурко, Д.В. Грознов, Г.А. Петров, О.П. Гаркин // Системы безопасности. – http://www.secuteck.ru/articles2/kompleks_sys_sec/pervyy-rubezh-ohrany-mneniya-ekspertov-ob-osobennostyah-ohrany-perimetra-v-gorodskoy-srede.

49 Программные миры: ПО для IP-видеонаблюдения на базе открытой архитектуры / Ф.М. Волковицкий, И.В. Фаломкин, М.С. Бабурин // Системы безопасности. – http://www.secuteck.ru/articles2/ip-security/programmnye-miry-po-dlya-ip-videonablyudeniya-na-baze-otkrytoy-arhitektury.

50 На чем стоит СКУД… / А.В. Гинце // Techportal.ru – http://www.techportal.ru/review/acs-large-enterprise.

ПРИЛОЖЕНИЕ А

Листинг 1

```
* Copyright (c) 2011. Philipp Wagner <bytefish[at]gmx[dot]de>.
 *
 * Является общественным достоянием в соответствии с лицензией BSD
 * Распространение и использование в исходной и двоичной формах с
 * модификацией или без нее допускается при условии соблюдения
 * следующих условий:
 *    - При распространении исходного кода необходимо сохранить
вышеуказанное
 * уведомление об авторских правах, этот список условий и следующий
отказ
 * от ответственности.
 *    - Распространение в двоичной форме должно
 * воспроизводить вышеуказанное уведомление об авторских правах, этот
 * список условий и следующее заявление об отказе от ответственности
в
 * документации и / или других материалах, предоставляемых с
распространением.
 *    - Ни имя организации, ни имена ее участников не могут
использоваться для
 * одобрения или продвижения продуктов, полученных из этого
программного
 * обеспечения без специального предварительного письменного
разрешения.
 * См. <Http://www.opensource.org/licenses/bsd-license>


 *   See <http://www.opensource.org/licenses/bsd-license>
 */


#include «stdafx.h»
#include «opencv2/core/core.hpp»
#include «opencv2/contrib/contrib.hpp»
#include «opencv2/highgui/highgui.hpp»

#include <iostream>
#include <fstream>
#include <sstream>

using namespace cv;
using namespace std;

static void read_csv(const string& filename, vector<Mat>& images,
vector<int>& labels, char separator = ';') {
    std::ifstream file(filename.c_str(), ifstream::in);
    if (!file) {
        string error_message = «No valid input file was given, please
check the given filename.»;
        CV_Error(CV_StsBadArg, error_message);
    }
    string line, path, classlabel;
```

```
    while (getline(file, line)) {
        stringstream liness(line);
        getline(liness, path, separator);
        getline(liness, classlabel);
        if(!path.empty() && !classlabel.empty()) {
            images.push_back(imread(path, 0));
            labels.push_back(atoi(classlabel.c_str()));
        }
    }
}

int main(int argc, const char *argv[]) {
    // Проверка на корректность указанных в командной строке
   // аргументов, печать подсказки, если аргументов нет.

    if (argc != 2) {
        cout << «usage: « << argv[0] << « <csv.ext>« << endl;
        exit(1);
    }
    // Путь к файлу CSV.
    string fn_csv = string(argv[1]);
    // Векторы ниже будут содержать изображения и соотв.им метки.
    vector<Mat> images;
    vector<int> labels;
    // Считывание данных

    try {
        read_csv(fn_csv, images, labels);
    } catch (cv::Exception& e) {
        cerr << «Ошибка открытия файла \»« << fn_csv << «\». Причина:
« << e.msg << endl;

        exit(1);
    }
    // Завершение, если на вход подано недостаточно изображений.
    if(images.size() <= 1) {
        string error_message = «Изображений недостаточно!»;
        CV_Error(CV_StsError, error_message);
    }
    // Получение высоты первого изображения. Это понадобится позже,
   // при восстановлении изображений в их оригинальном размере.
    int height = images[0].rows;

    Mat testSample = images[images.size() - 1];
    int testLabel = labels[labels.size() - 1];
    images.pop_back();
    labels.pop_back();
    // Строки ниже создают модель LBPH для распознавания и тренируют
   // ее поданной на вход серией изображений.
    //
   // Созданная модель имеет следующие значения по умолчанию:
    //
    //      radius = 1
    //      neighbors = 8
    //      grid_x = 8
```

```
    //      grid_y = 8
    //
    // Значения можно менять, подавая их на вход модели:
    //      cv::createLBPHFaceRecognizer(2, 16);
    //
    //
    //
    Ptr<FaceRecognizer> model = createLBPHFaceRecognizer();
    model->train(images, labels);
    // Строка ниже присваивает переменную для хранения значения
результата распознавания:
    int predictedLabel = model->predict(testSample);
    //
    // Для изменения уверенности распознавания нужно в присвоении
  // выше указать такие параметры:
    //
    //      int predictedLabel = -1;
    //      double confidence = 0.0;
    //      model->predict(testSample, predictedLabel, confidence);
    //
    // Интерпретация результатов распознавания и вывод сообщения о
соответствии\несоответствии
   string result_message = format(«Predicted class = %d / Actual
class = %d.», predictedLabel, testLabel);
    cout << result_message << endl;

    return 0;
}
```

ПРИЛОЖЕНИЕ Б

1 270304.2018.850.01.01 Д1, «Автоматизированная система контроля доступа на производственное предприятие Челябинское ЛПУ. Алгоритм действий по подготовке входной информации для модуля распознавания лиц».

2 270304.2018.850.01.01 Д2, «Автоматизированная система контроля доступа на производственное предприятие Челябинское ЛПУ. Алгоритм сценария «Распознавание лиц».

3 270304.2018.850.02.01 С1, «Автоматизированная система контроля доступа на производственное предприятие Челябинское ЛПУ. Схема структурная».