# Содержание

Введение.....3

1 Теоретические основы обеспечения авиационной безопасности в аэропорту .....5

1.1 Нормативно-правовое регулирование обеспечения охраны и безопасности аэропортов.....5

1.2 Современные проблемы обеспечения авиационной безопасности в аэропорту.....11

2 Анализ перспективных средств контроля доступа в аэропортах.....15

2.1 Цели и задачи СКУД в аэропортах.....15

2.2 Организация контрольно-пропускных пунктов в аэропорту.....17

2.3 Перспективы внедрения биометрических систем контроля доступа.....21

Заключение.....25

Список использованных источников.....27

# Введение

Интенсификация транспортной отрасли, эволюционное развитие транспортных систем ставят новые задачи в вопросах транспортной безопасности.

Чем более сложные системы создаются для обеспечения процессов в аэропортах, чем выше скорости передвижения, пассажиров и грузопоток, тем более сложные задачи приходится решать в области транспортной безопасности.

Основным подразделением аэропорта, ответственным за предотвращение актов незаконного вмешательства (АНВ) в деятельность гражданской авиации, является служба авиационной безопасности (САБ).

Данная служба требует особого внимания, так как с каждым годом техническое оснащение террористических группировок улучшается, а финансовая мощь увеличивается, что дает им возможность разрабатывать более мощное и универсальное оружие.

Именно поэтому неотъемлемой частью САБ является досмотр пассажиров, личных вещей при пассажирах, багажа, грузов, почты, бортовых запасов, а так же членов экипажей и авиационного персонала. Досмотру подвергаются все лица и транспортные средства, попадающие в контролируемую зону аэропорта.

2022 год стал годом потрясений и серьезных кризисных явлений в гражданской авиации Российской Федерации.

Действующие ограничения на выполнения международных полетов, очевидно, снизили нагрузку на службу авиационной безопасности, вместе с тем неблагоприятная геополитическая обстановка способствует тому, что

возросла угроза актов незаконного вмешательства и террористических актов на воздушном транспорте.

В связи с этим можно сделать вывод о том, что тема курсовой работы «Инновационные средства в системе контроля доступа» является актуальной для исследования.

Целью курсовой работы является разработка предложений по обеспечению авиационной безопасности при проведении эксплуатационных мероприятий в аэропорту "Пулково"

Для достижения поставленной цели работы необходимо решить следующий перечень задач:

- рассмотреть понятие эксплуатационных мероприятий;

- изучить нормативно-правовые документы, регламентирующие деятельности службы авиационной безопасности;

- охарактеризовать современные способы обеспечения авиационной безопасности при проведении эксплуатационных мероприятий.

- проанализировать особенности обеспечения контроля доступа в аэропортах;

- разработать предложения по внедрению инновационных средств в системе контроля доступа.

Цели и задачи данной работы определили ее структуру. Курсовая работа состоит из введения, основной части, заключения и списка использованных источников.

Объектом исследования курсовой работы является процесс обеспечения контроля доступа в зоны аэропорта.

Предмет исследования – процесс внедрения инновационных средств в систему контролю доступа.

Практическая значимость данного исследования обусловлена тем, что в условиях увеличения угрозы АНВ разработанные предложения по по

внедрению инновационных средств в системе контроля доступа будут способствовать повышению уровня безопасности.

# 1 Теоретические основы обеспечения авиационной безопасности в аэропорту

## 1.1 Нормативно-правовое регулирование обеспечения охраны и безопасности аэропортов

Первым этапом выполнения исследования курсовой работы является изучение системы нормативных требований, регламентирующих порядок и проведение процедур по обеспечению авиационной безопасности в аэропортах Российской Федерации.

Одними из основных объектов террористических акций являются аэропорты. Несмотря на то, что в последние годы на воздушном транспорте применяются новейшие средства обеспечения безопасности - возможность совершения терактов в этой области сохраняется.

Для надежного функционирования аэропортов должна быть обеспечена комплексная безопасность, наиболее важной составляющей которой является инженерно-техническая система безопасности, которая позволяет обеспечить надежную защиту любого объекта, а также обнаружить и нейтрализовать террористические угрозы практически при любых условиях и сценариях развития событий. Мировой опыт убедительно показывает, что одно только применение надежных технических средств охраны, созданных на базе новейших технологий, позволяет существенно снизить процент террористических посягательств на охраняемые объекты.

Важнейшим шагом в обеспечении авиационной безопасности и защиты международных аэропортов от террористических актов и иных противоправных посягательств является устройство ограждений по периметру основной территории аэропорта и периметрам его жизненно важных центров.

Основные требования, предъявляемые к техническим средствам авиационной безопасности, регламентированы Приказом Минтранса РФ от 18.04.2008 N 62 (ред. от 10.03.2011) "Об утверждении Программы авиационной безопасности гражданской авиации Российской Федерации".

В соответствии с данным нормативным актом для обеспечения требуемого уровня авиационной безопасности аэропорты, аэродромы должны быть оборудованы следующими техническими средствами авиационной безопасности:

1) для защиты от несанкционированного проникновения посторонних лиц и транспортных средств в контролируемую зону и на объекты инфраструктуры аэропорта - инженерно-техническими средствами охраны:

- защитные ограждения, тревожная и охранная сигнализация,

- контрольно-пропускные пункты с техническими и специальными средствами досмотра персонала и специальными устройствами для досмотра транспортных средств и грузов,

- система видеонаблюдения с записью видеоизображения;

2) для проведения досмотра пассажиров, багажа, вещей, находящихся при пассажирах, членов экипажей воздушных судов, авиационного персонала, грузов и почты, бортовых запасов воздушного судна и бортового питания - техническими и специальными средствами досмотра (стационарные рентгенотелевизионные интроскопы и металлоискатели;

- рентгенографические томографы;

- рентгенографические сканеры; системы сканирования, работающие на принципе контроля активных миллиметровых волн, являющихся обычными радиочастотными сигналами; системы интровидения в терагерцевом диапазоне электромагнитного спектра; системы ядерного квадрупольного резонанса;

- портативные (ручные) металлоискатели; средства для обнаружения паров или частиц взрывчатых веществ и другие средства), системами видеонаблюдения с записью видеоизображения.

Для защиты воздушных судов от несанкционированного проникновения на борт посторонних лиц, захвата и угона применяются:

- штатные противоугонные устройства с тревожной сигнализацией;

- надежно запирающиеся с внутренней стороны кабины экипажа пуленепробиваемые двери и перегородки, изолирующие пилотскую кабину от пассажирского салона;

- специальные сигнализационные и переговорные устройства для связи командира воздушного судна и бортпроводников (бортовых операторов);

- телевизионные системы наблюдения за обстановкой в пассажирских салонах, кабине летного экипажа и средствами контроля с рабочего места каждого пилота всей зоны двери с внешней стороны кабины летного экипажа с возможностью передачи аудио-, видео информации в реальном масштабе времени по каналам спутниковой связи в наземные центры управления.

Эксплуатация инженерно-технических средств охраны, технических и специальных средств досмотра осуществляется в соответствии с рекомендациями изготовителя и индивидуальными стандартными эксплуатационными процедурами, содержащимися в программе обеспечения авиационной безопасности аэропортов, авиационных предприятий и эксплуатантов.

Организации гражданской авиации, эксплуатирующие технические средства охраны, технические и специальные средства досмотра, разрабатывают графики профилактического технического обслуживания и ремонта средств в целях поддержания оптимальной эффективности их работы.

Для поддержания постоянной работоспособности технических средств охраны, технических и специальных средств досмотра их эксплуатация осуществляется специально подготовленными сотрудниками службы авиационной безопасности, а техническое обслуживание осуществляется специалистами, имеющими соответствующую квалификацию.

Еще одним документом, в котором описаны технические средства контроля доступа и инженерно-технические средства охраны, является ГОСТ Р 55250-2012 Национальный стандарт РФ «АЭРОПОРТЫ. ТЕХНИЧЕСКИЕ СРЕДСТВА КОНТРОЛЯ ДОСТУПА И ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ».

Данный стандарт распространяется на инженерно-технические средства охраны и технические средства контроля и управления доступом, предназначенные для исключения несанкционированного доступа людей и транспорта в (из) контролируемую зону аэропорта и объекты его инфраструктуры, а также контроля и санкционирования доступа.

Стандарт устанавливает общие технические требования к инженерно-техническим средствам охраны и техническим средствам контроля и управления доступом. Данный стандарт распространяется на вновь разрабатываемые и модернизируемые средства и системы контроля и управления доступом.

Рассмотрим некоторые особенности обеспечения аэропорта средствами охраны и безопасности в соответствии с данным нормативным документом.

Автономные системы КУД должны обеспечивать:

- открывание 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 пожарной безопасности;

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

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

Системы КУД должны 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 УУ;

- число и вид временных интервалов доступа (окон времени), уровней доступа;

- число 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 (требование обязательно для СКУД с биометрической идентификацией, для остальных допускается не указывать);

- показатели по уровням устойчивости к НСД.

УПУ должны обеспечивать:

- полное или частичное перекрытие проема прохода;

- ручное, полуавтоматическое или автоматическое управление;

- блокирование человека или объекта для УПУ блокирующего типа.

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.

Для УПУ должна быть предусмотрена возможность механического аварийного открывания в случае отключения электропитания, при пожаре или других стихийных бедствиях. Аварийная система открывания должна быть защищена от возможности использования ее для несанкционированного проникновения.

Считыватели УВИП должны обеспечивать:

- возможность считывания идентификационного признака с идентификаторов;

- введение биометрической информации (для считывателей биометрической информации);

- преобразование введенной информации в электрический сигнал;

- передачу информации на УУ.

УВИП должны быть защищены от манипулирования путем перебора и подбора идентификационных признаков. Виды защиты должны быть указаны в стандартах и (или) технических условиях на УВИП конкретного типа.

Идентификаторы УВИП должны обеспечивать хранение идентификационного признака в течение срока службы и при эксплуатации.

Конструкция, внешний вид и надписи на идентификаторе и считывателе не должны приводить к раскрытию применяемых кодов.

Аппаратные средства УУ должны обеспечивать прием информации от УВИП, обработку информации и выработку сигналов управления на исполнительные устройства УПУ.

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.

Виды и параметры протоколов и интерфейсов должны быть установлены в стандартах и технических условиях на УУ конкретного типа с учетом требований ГОСТ 26139.

Таким образом, в данном разделе работы были рассмотрены требования нормативных документов, предъявляемые к средств охраны и безопасности аэропортов, предназначенные для организации антитеррористического благополучия населения.

## 1.2 Современные проблемы обеспечения авиационной безопасности в аэропорту

Ранее было установлено, что в настоящее время системы технической эксплуатации зданий и сооружений можно рассматривать как совокупность взаимосвязанных организационных и технических мероприятии по установлению технического состояния зданий и сооружений, проведению профилактических мер и ремонтов конструкций и оборудования, осуществляемых в строго установленные сроки, для обеспечения сохранности и эксплуатационной пригодности, предупреждения преждевременного износа и предотвращения аварийных ситуации.

В то же время выполнение любых работ, не связанных с обеспечением перевозок, выходит за привычные рамки контура управления авиационной безопасностью, поэтому возникают дополнительные задачи по обеспечению авиационной безопасности при проведении эксплуатационных мероприятий в аэропорту.

Контроль безопасности на таких стратегических инфраструктурных объектах, как аэропорты, – сложная задача, с которой может справиться далеко не каждая частная охранная компания. Для обеспечения нормального и бесперебойного функционирования гражданской авиации законодательно установлен порядок охраны таких объектов.

Речь идёт не только о безопасности персонала и пассажиров, но и о невмешательстве в режим работы аэропорта со стороны злоумышленников. Таким образом, базовая функция службы охраны заключается в предотвращении и препятствовании несанкционированному доступу на территорию объекта, в том числе с проносом оружия, взрывчатки и иных предметов, которые представляют или могут представлять потенциальную опасность для людей, оборудования и лётной техники.

За безопасность аэропорта по закону отвечает администрация, которая осуществляет эксплуатацию и обслуживание инфраструктурного объекта. В первую очередь речь идёт об охране периметра и входов в здание с целью выявления и предотвращения любых попыток незаконного проникновения на территорию аэропорта.

Охрана зданий и сооружений аэропорта при проведении эксплуатационных мероприятий происходит по тем же стандартам, что и охрана любого крупного инфраструктурного объекта с большим потоком посетителей. Служба безопасности берет на себя следующие функции:

1. Патрулирование зданий аэропорта и прилегающих территорий.
2. Обеспечение работы стационарных пунктов охраны.
3. Видеомониторинг помещений аэропорта и близлежащих территорий.
4. Обеспечение пропускного режима и досмотр посетителей.

Гораздо более сложная задача – это охрана периметра аэропорта, особенно, при проведении эксплуатационных мероприятий, таких как уборка дорог, покраска заборов, а также при любых ремонтных работах вблизи контролируемого контура.

Учитывая, что длина взлетно-посадочных полос измеряется несколькими километрами, а вся площадь аэропорта составляет сотни гектаров, служба безопасности в лице сотрудников САБ должна иметь достаточную квалификацию, чтобы обеспечить защиту на должном уровне.

Естественно, охрана большого объекта с привлечением частных охранных организаций с учетом специфики задачи – весьма дорогостоящее мероприятие. Тем не менее, если служба безопасности аэропорта не способна организовать качественную охрану собственными силами, частная охранная компания привлекается в обязательном порядке. Такая практика применима в большинстве международных аэропортов России.

Как объект охраны аэропорт имеет свою специфику. В частности, повышенный уровень электромагнитных излучений выставляет определённые требования к рабочим параметрам технических средств защиты. Также в аэропорту непрерывно находится большое количество людей вне зависимости от времени суток. Это обязывает охрану работать в режиме максимальной эффективности 24 часа, 7 дней в неделю. Определённые требования к организации системы безопасности диктует и тот факт, что аэропорт как стратегический инфраструктурный объект функционирует непрерывно.

Для охраны периметра аэропорта в аэропорту применяется специальное оборудование. Практика показывает, что глухого ограждения в виде бетонного забора вдоль всей территории недостаточно, чтобы исключить несанкционированное проникновение на взлётно-посадочные полосы и другие охраняемые объекты. Что касается патрулирования периметра, то этот метод ещё более затратный и применяется как

дополнительная мера безопасности, создающая возможность для оперативного реагирования на любые угрозы.

Именно поэтому основные функции безопасности периметра ложатся на современные технические средства защиты. Такие системы дают возможность в режиме реального времени отслеживать вверенный объект и фиксировать малейшие попытки нарушения охраняемых границ третьими лицами.

К оборудованию для охраны периметра при проведении эксплуатационных мероприятий предъявляются жесткие требования, среди которых:

- бесперебойная работа техники в условиях пересечённой местности;

- отсутствие или минимизация неконтролируемых «слепых» зон;

- стойкость к агрессивному воздействию внешних атмосферных факторов;

- эффективность мониторинга при интенсивных паразитных помехах и радиопомехах;

наличие активных алгоритмов отслеживания и обработки тревожных сигналов.

Существует масса средств по обеспечению контроля периметра аэропорта. Одними из наиболее передовых и эффективных методов считаются оптоволоконные системы безопасности.

Их преимущество заключается в том, что они идеально приспособлены для контроля больших территорий, измеряемых десятками километров. Ещё один плюс – высокая пожаробезопасность оптоволоконного сенсора, что особенно важно на крупных инфраструктурных объектах.

Таким образом, специфичность задачи защиты аэропорта во время проведения эксплуатационных мероприятий, которая ставится перед службой авиационной безопасности, заключается в необходимости контролировать большую территорию, обеспечивая при этом бесперебойное функционирование гражданской авиации.

# 2 Анализ перспективных средств контроля доступа в аэропортах

## 2.1 Цели и задачи СКУД в аэропортах

Внедрение в аэропорту системы безопасности необходимо, прежде всего, для обеспечения бессбойной работы всей инфраструктуры аэропорта, устранения влияния внешних угроз на имущество, сотрудников и пассажиров, а также предотвращения злоупотреблений среди служащих аэропорта.

Со всеми этими задачами может должным образом справиться только комплексная система, включающая подсистемы видеонаблюдения, пожаробезопасности, контроля и управления доступом, бортовой безопасности самолетов и другие системы – находящиеся, разумеется, под чутким и надежным управлением различных подразделений службы безопасности.

Система контроля и управления доступом (далее – СКУД) отвечает, главным образом, за поддержку контрольно-пропускного режима на территории аэропорта, а это связано с разграничением прав доступа персонала к помещениям и объектам, учетом въезда-выезда автотранспорта, учетом пассажиропотока, досмотром багажа и хранением данных о часто летающих пассажирах.

Последняя возможность обрела новую жизнь, главным образом, в зарубежных аэропортах международного значения с повсеместным внедрением биометрического оборудования. Главная задача этой системы – оградить инфраструктуру и имущество аэропорта и находящихся на его территории людей от внешней угрозы, что бы она собой ни представляла. Соответственно, оборудование контроля доступа устанавливается на внешние входы и въезды автотранспорта, и посты охраны, контрольно-

пропускные пункты (КПП), а также некоторые служебные помещения аэропорта.

Прежде чем говорить о структуре и необходимом функционале СКУД, следует более детально очертить круг задач, за решение которых на территории аэропорта отвечает эта система.

Задачи:

- Автоматизация работы проходных с возможностью учета рабочего времени сотрудников.

- Автоматизация КПП и интеграция с парковочными системами с возможностью фиксации автомобильных номеров, автоматизации оплаты парковки, распределения автомобилей по свободным парковочным местам.

- Разграничение доступа к помещениям и объектам аэропорта с присвоением сотрудникам разных прав доступа. Актуально введение разных временных зон, разных правил прохода в помещения. Доступ может осуществляться по карте, по набору кода, по уникальным биометрическим данным. Чаще всего при доступе к особо охраняемым помещениям необходимой мерой является режим многофакторной идентификации с проверкой разных идентификационных данных.

- Обеспечение сохранности имущества и отслеживание его перемещения как на территории аэропорта, так и за его пределами может осуществляться с помощью радиометок, а в случае транспортных средств – с помощью GPS/GSM-модулей.

- Досмотр имущества пассажиров и въезжающего на территорию аэропорта транспорта с целью выявления потенциально опасных предметов и веществ (оружия, взрывчатки, горючих веществ и проч.)

СКУД аэропорта должна включать в себя следующие компоненты:

- Персональные идентификаторы (как правило, в качестве идентификаторов применяются бесконтактные проксимити-карты или смарт-карты, однако для ограничения доступа к отдельным объектам все чаще используются биометрические идентификаторы)

- Считыватели персональных идентификаторов (в зависимости от типа используемых идентификаторов, это могут быть считыватели проксимити- или смарт-карт, а также биометрические считыватели – чаще всего считыватели отпечатков пальцев с возможностью идентификации по карте).

- Контроллеры замков, турникетов, других исполнительных устройств СКУД. С целью повышения живучести системы СКУД проектируют таким образом, чтобы данные о персональных идентификаторах и соответствующих им правах доступа хранилась в энергонезависимой памяти контроллеров.

- Исполнительные устройства дверных замков, турникетов; электрические приводы ворот и шлагбаумов.

- Систему распознавания государственных регистрационных номеров автотранспорта.

- Автоматизированные рабочие места – АРМ (о них речь пойдет отдельно).

## 2.2 Организация контрольно-пропускных пунктов в аэропорту

В первую очередь, в данном разделе работы предлагается рассмотреть функции и режимы работы СКУД, необходимых для правильной организации этого жизненно важного объекта аэропорта.

Каждый КПП в аэропорту должен быть оснащен системой видеонаблюдения, позволяющей контролировать зону прохода через металлодетектор или проем ворот, а также средствами СКУД, обеспечивающими контроль прохода пользователей (пассажиров). КПП контролирующие проезд автомобилей оснащаются также системой считывания номеров, шлагбаумом и средствами индикации разрешения на въезд-выезд (световые табло, светофоры). Кроме того, такие КПП обязательно должны быть оборудованы дополнительными средствами

защиты от несанкционированного проникновения транспортных средств при взломанном шлагбауме.

Выезд на перрон оборудуется средствами контроля над проходом и проездом с учетом того, что соответствующий КПП находится на открытом пространстве. Контроль проезда автотранспорта осуществляется с помощью радиочастотных меток. Аналогичным образом осуществляется контроль при въезде на базовый склад ГСМ.

Системы контроля доступа для КПП должна обеспечивать выполнение следующих функций:

1. Контроль реального прохода/въезда на территорию аэропорта

Во-первых, СКУД на КПП аэропорта должна осуществлять контроль за фактом реального прохода пассажира или встречающего/провожающего, а также проезда автотранспорта на территорию аэропорта. При типовой организации КПП сначала происходит идентификация проходящего контроль путем регистрации электронного пропуска (идентификатора). При этом пересечение КПП считается осуществленным (т.е. имеет место факт реального прохода) только в случае фиксации прохода, к примеру, проворотом турникета. В противном случае проход считается незавершенным.

Практически аналогичен учет проезжающего на территорию аэропорта автотранспорта. Проезд считается зафиксированным фактом только после пересечения автотранспортом лучей датчиков либо индукционных петель. В ином случае фиксируется незавершенная попытка проезда.

2. Запрет повторного прохода/проезда в рамках всей СКУД

В случае, если происходит повторная регистрация электронного пропуска, а выход/выезд с территории аэропорта перед этим зарегистрирован не был, то сотрудники охраны вправе отказать проходящему в доступе на территорию аэропорта. То же правило может распространяться и на отдельные помещения на территории аэропорта.

3. Поддержка многосменных и скользящих графиков работы

В целях безопасности имеет смысл обеспечить допуск персонала на территорию аэропорта только в рабочее время, а вне работы учитывать каждого сотрудника как рядового посетителя. Для этого контроллеры СКУД, расположенные на проходных и КПП, должны поддерживать работу с многосменными и скользящими графиками. К тому же, это позволит снять часть нагрузки с сотрудников КПП.

4. Оперативное присвоение прав прохода через КПП

В экстренных ситуациях, которые, к сожалению, нередко случаются в жизни любого аэропорта, может возникнуть необходимость экстренного вызова сотрудников с нарушением рабочего графика, заложенного в память контроллеров. В этом случае, чтобы избежать нахождения на территории аэропорта неучтенных лиц, которых диспетчер КПП пропустил нажатием кнопки разблокирования турникета, в СКУД должен поддерживаться режим экстренного присвоения прав доступа диспетчеру КПП. Это событие должно регистрироваться в БД СКУД.

5. Распознавание государственных регистрационных номеров

В качестве идентификатора транспортного средства может выступать его государственный регистрационный номер. По нему диспетчер может получить из БД всю ранее зафиксированную информацию с отметкой о том, разрешено ли данному автомобилю проезжать через КПП. Как и в случае с другими идентификаторами, окончательно решение о допуске транспортного средства на территорию аэропорта может быть возложено на плечи диспетчера. Эта система удобна и автоматически снимает ряд вопросов, связанных с традиционными идентификаторами – выбор типа идентификатора (в том числе для разовых посетителей), процедуры их выдачи и сдачи, контроль ответственность за утерю идентификатора.

6. Автоматический ввод фотографий автомобилей

Еще одна полезная и удобная, но не обязательная функция. В случае ее использования при первом проезде автомобиля через КПП в БД СКУД автоматически вводится его мгновенный снимок с обзорной телекамеры,

установленной над въездом. При последующих проездах эта фотография, выводимая из БД вместе с другой информацией об автомобиле, может быть использована для верификации.

7. Двери (или функции СКУД для пассажиров)

Для здания аэропорта, двери – это не просто створки, через которые можно (или нельзя – в зависимости от прав доступа) войти в какое-либо помещение. Эти створки, чем бы они не были представлены (турникеты, шлюзовые кабины и т.д.), должны привлекательно выглядеть, защищать помещение от воздействия окружающей среды и обладать высокой пропускной способностью, дабы не скапливались перед ними очереди из граждан с багажом.

Помимо комфорта и удобства пассажиров и персонала, двери должны стоять еще и на страже безопасности аэропорта. Поэтому при их изготовлении предусматривают наличие пожарозащищености, специального остекления, а также возможность экстренного открытия дверей в случае ЧП или при эвакуации пассажиров. Кроме того, уже на этапе производства закладывается возможность работы двери в составе системы безопасности.

За годы успешной, в целом, эксплуатации СКУД на территории аэропортов сложились своего рода правила подбора дверей, турникетов и проч. для разных помещений. Если не правила, то, по крайней мере, классические рекомендации.

8. Стойки паспортного контроля

Для организации прохода пассажиров по направлению к стойкам используются таможенные коридоры и система перемещения грузов. В этих случаях наилучшим вариантом считается применение автоматических распашных калиток и трехштанговых турникетов (типа «трипод»).

9. VIP-зона

В VIP-зоне ожидают начала посадки пассажиры первого и бизнес-классов. В традиционном варианте этот зал охраняется людьми в форме,

которые на основе посадочных талонов решают, кого пустить внутрь, а кого попридержать.

Однако все чаще и чаще вместо постов охраны на входе в VIP-зону устанавливаются раздвижные двери различной конфигурации и дизайна.

Иногда используются шлюзовые кабины. Внутренние двери кабины не закроются, пока открыты внешние. Для защиты помещения от задымления конструкция дверей должна предусматривать дымоудаление. Хорошо, если дверь (или шлюзовая кабина) изготовлена из непрозрачных материалов, позволяющих скрыть внутреннее пространство. Войти в VIP-зону можно при помощи посадочного талона, данные с которого считывает установленный рядом с входом считыватель СКУД.

10. Проход на посадку

Поскольку на посадку пассажиры обычно идут довольно плотным потоком, на помощь сотрудникам аэропорта на этом участке могут прийти терминалы, оборудованные блоками автоматизированного учета. После считывания информации с посадочного талона турникет разблокируется. Использование автоматизированного учета пассажиров может значительно сократить время посадки.

На этом участке наиболее приемлемо применение турникетов типа «трипод». Он удобен в применении и быстро переходит в следующую позицию. При прохождении пассажира после несильного толчка рукой штанга турникета проворачивается, переходя в следующее положение. Если на посадку проходит группа пассажиров или осуществляется транзит груза, то штанга турникета опускается при нажатии кнопки. При необходимости срочной эвакуации возможность такого «падения» штанги обеспечивает эвакуационный коридор.

## 2.3 Перспективы внедрения биометрических систем контроля доступа

Биометрические технологии основаны на биометрии, измерении уникальных характеристик отдельно взятого человека.

Это могут быть как уникальные признаки, полученные им с рождения, например: ДНК, отпечатки пальцев, радужная оболочка глаза; так и характеристики, приобретённые со временем или же способные меняться с возрастом или внешним воздействием. Например: почерк, голос или походка.

Основным способом защиты информации от злоумышленников считается внедрение так называемых средств ААА, или 3А (authentication, authorization, administration - аутентификация, авторизация, администрирование).

Среди средств ААА значимое место занимают аппаратно-программные системы идентификации и аутентификации (СИА) и устройства ввода идентификационных признаков (термин соответствует ГОСТ Р 51241-98), предназначенные для защиты от несанкционированного доступа (НСД) к компьютерам.

При использовании СИА сотрудник получает доступ к компьютеру или в корпоративную сеть только после успешного прохождения процедуры идентификации и аутентификации.

Идентификация заключается в распознавании пользователя по присущему или присвоенному ему идентификационному признаку. Проверка принадлежности пользователю предъявленного им идентификационного признака осуществляется в процессе аутентификации.

В состав аппаратно-программных СИА входят идентификаторы, устройства ввода-вывода (считыватели, контактные устройства, адаптеры, платы доверенной загрузки, разъемы системной платы и др.) и соответствующее ПО.

Идентификаторы предназначены для хранения уникальных идентификационных признаков. Кроме того, они могут хранить и обрабатывать разнообразные конфиденциальные данные. Устройства ввода-

вывода и ПО пересылают данные между идентификатором и защищаемым компьютером.

Биометрическая идентификация – это способ идентификации личности по отдельным специфическим биометрическим признакам (идентификаторам), присущим конкретному человеку.

Биометрическая аутентификация - это опознание индивидуума на основе его физиологических характеристик и поведения. Аутентификация проводится посредством компьютерной технологии без какого-либо нарушения личной сферы человека.

Собранные таким образом в базе данных приметы человека сравниваются с теми, которые актуально регистрируются системами безопасности.

Функции:

1. Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем называется идентификацией.

Идентификация обеспечивает выполнение следующих функций:

- установление подлинности и определение полномочий субъекта при его допуске в систему,

- контролирование установленных полномочий в процессе сеанса работы;

- регистрация действий и др.

Аутентификацией (установлением подлинности) называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Биометрические технологии активно применяются во многих областях связанных с обеспечением безопасности доступа к информации и материальным объектам, а также в задачах уникальной идентификации личности.

Применения биометрических технологий разнообразны: доступ к рабочим местам и сетевым ресурсам, защита информации, обеспечение доступа к определённым ресурсам и безопасность.

Ведение электронного бизнеса и электронных правительственных дел возможно только после соблюдения определённых процедур по идентификации личности.

Биометрические технологии используются в области безопасности банковских обращений, инвестирования и других финансовых перемещений, а также розничной торговле, охране правопорядка, вопросах охраны здоровья, а также в сфере социальных услуг.

Биометрические технологии в скором будущем будут играть главную роль в вопросах персональной идентификации во многих сферах. Применяемые отдельно или используемые совместно со смарт-картами, ключами и подписями, биометрия скоро станет применяться во всех сферах экономики и частной жизни.

# Заключение

Таким образом, в курсовой работе были проанализированы особенности установления режима контролируемого доступа в аэропортах, а также расмотрены новые технологии в области обеспечения доступа.

В заключение можно отметить, что наиболее перспективным направлением в области контроля доступа становятся нейронные сети.

По данной технологии нейросеть-детектор принимает поток изображений с видеокамеры и определяет, есть ли там лица. Набор лиц она подает на вход нейросети-идентификатору, которая сравнивает их с базой данных лиц-эталонов и говорит, есть совпадение или нет.

Как и мозг, нейросеть оперирует признаками. Есть математическая модель, преобразующая изображение лица в список признаков. Перебирая варианты, можно менять структуру этой модели, чтобы улучшить результат. Задача нейросети сводится к преобразованию изображения в набор признаков. Делает она это с помощью фильтров в виде математических формул.

Чтобы нейросеть успешно распознавала лица, ее нужно обучить на большой базе изображений. Это долгий процесс с множеством итераций. В зависимости от размера базы и вычислительных ресурсов на это уходят недели и месяцы. Шаг за шагом система учится все точнее распознавать лица. Программисты только следят за тем, чтобы векторы признаков (результат работы нейросети) были максимально информативными, позволяли проводить сравнение.

Для обученной нейросети не представляют проблем возраст, пол, этническая принадлежность лица. Она способна за считаные секунды дать ответ на вопрос, кто из этих десяти миллионов находился в поле зрения полутора тысяч камер. Человек не сделает такого никоим образом.

Одна из актуальных задач — организация автоматического доступа в контролируемые зоны аэропорта. Нейронная сеть в режиме реального времени сравнивает людей, попавших в поле зрения камер, с находящимися в базе данных аэропорта.

При совпадении информация моментально передается на сервер, и тот дальше передает сигнал на открытие двери. Это позволяет повысить уровень безопасности в аэропорту.

# Список использованных источников

1. Федеральный закон Российской Федерации от 19.03.1997 г. № 60-ФЗ «Воздушный кодекс Российской Федерации».

2. Федеральный закон Российской Федерации от 09.02.2007 г. № 16-ФЗ «О транспортной безопасности»

3. Закон Российской Федерации «О Государственной границе Российской Федерации» от 01.04.1993 № 4730-1

4. Закон Российской Федерации «О ведомственной охране» от 14.04.1999 № 77-ФЗ, принят Государственной Думой 12.03.99, одобрен Советом Федераций 31.03.1999.

5. Закон Российской Федерации «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с осуществлением мер авиационной безопасности на воздушном транспорте» от 21.03.2005 № 20-ФЗ.

6. Закон Российской Федерации «О противодействии терроризму» от 06.03.2006 № 35-ФЗ.

7. Указ Президента Российской Федерации от 15.02.2006 № 116 «О мерах по противодействию терроризму». (Положение о Национальном антитеррористическом комитете).

8. Постановление Правительства Российской Федерации РФ от 30.07.1994 г. № 897 «О Федеральной системе обеспечения защиты деятельности гражданской авиации от актов незаконного вмешательства».

9. Постановление Правительства Российской Федерации от 10.12.2008 г. № 940 «Об уровнях безопасности объектов транспортной инфраструктуры и транспортных средств и о порядке их объявления (установления)».

10.Постановление Правительства Российской Федерации «О мерах по противодействию терроризму» от 15.09.1999 № 1040.

11.Постановление Правительства РФ от 22.12.2006 № 784 «Об утверждении Положения о лицензировании деятельности по обеспечению авиационной безопасности».

12.Распоряжение Правительства Российской Федерации от 05.11.2009 г. № 1653-р «Об утверждении Перечня работ, непосредственно связанных с обеспечением транспортной безопасности».

13.Приказ Минтранса России от 28.11.2005 N 142 (ред. от 12.02.2018) "Об утверждении Федеральных авиационных правил "Требования авиационной безопасности к аэропортам" (Зарегистрировано в Минюсте России 28.12.2005 N 7321).

14.Приказ Министерства транспорта Российской Федерации от 11.02.2010 г. № 34 «Об утверждении порядка разработки планов обеспечения транспортной безопасности объектов транспортной инфраструктуры и транспортных средств».

15.Приказ Министерства транспорта Российской Федерации, Федеральной службы безопасности России, Министерства внутренних дел Российской Федерации от 05.03.2010г. № 52/112/134 «Об утверждении Перечня потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств».

16.Приказ Министерства транспорта Российской Федерации от 08.02.2011 г. № 40 «Об утверждении Требований по обеспечению транспортной безопасности, учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств воздушного транспорта».

17.Приказ Министерства транспорта Российской Федерации от 20.07.2007 г. №104 « Об утверждении Правил проведения предполетного и послеполетного досмотров»

18.Приказ Министерства транспорта Российской Федерации от 20.01.1998 г. №22 «Об утверждении и введении в действие положения о

пропускном и внутриобъектовом режиме в аэропортах, авиапредприятиях, организациях и учреждениях ГА».

19.Алфимцев А.Н., Лычков И.И. Метод обнаружения объекта в видеопотоке в реальном времени // Вестник ТГТУ.- 2011.- Т. 17.- № 1

20.Брилюк Д.В., Старовойтов В.В. Распознавание человека по изображению лица нейросетевыми методами. - Минск, 2002.

21.Козлов В.А., Потапов А.С. Анализ методов выделения движущихся объектов на видеопоследовательностях с шумами // Научно-технич. вестник СПГУ ИТ. - 2011. - № 3 (73)

22.FaceVACSTechnology. B6T8 Algorithm Performance. http://www.cognitec-systems.de/fileadmin/cognitec/media/technology/FaceVACS-biometric-performance-b6t8.pdf.

23.http://www.emgu.com Сайт о Emgu CV

24.http://www.aforgenet.com Сайт для разработчиков и исследователей в области компьютерного зрения

25.http://www.cognitec-systems.de Сайт программного продукта FaceVACS

26.http://research.microsoft.com Сайт об исследованиях компании Microsoft

27.http://software.intel.com Сайт компании Intel

28.http://www.neurotechnology.com Ресурс о нейронных сетях