

**БЕЛГОРОДСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ
ИМЕНИ И.Д. ПУТИЛИНА**

**Использование систем
видеонаблюдения и видеоаналитики
для обеспечения безопасности
на объектах транспортной инфраструктуры
(аэропорты)**

Учебное пособие

**Белгород
Белгородский юридический институт МВД России
имени И.Д. Путилина
2018**

УДК 004: 351.749
ББК 67.401.133.12
И 88

Печатается по решению
редакционно-издательского совета
Бел ЮИ МВД России
имени И.Д. Путилина

Авторы: **Жукова П.Н.**, доктор физико-математических наук, доцент;
Прокопенко А.Н., кандидат технических наук, доцент; **Насонова В.А.**, канди-
дат физико-математических наук, доцент; **Дрога А.А.; Гуржий А.А.**

И 88 **Использование систем видеонаблюдения и видеоаналитики для
обеспечения безопасности на объектах транспортной инфраструкту-
ры (аэропорты) : учебное пособие / П. Н. Жукова [и др.]. – Белгород :
Бел ЮИ МВД России имени И.Д. Путилина, 2018. – 73 с.**

ISBN 978-5-91776-225-8

Рецензенты:

Линьков В.В., кандидат технических наук (Орловский юридический ин-
ститут МВД России имени В.В. Лукьянова);

Ходякова Н.В., доктор педагогических наук, доцент (Волгоградская ака-
демия МВД России).

В пособии рассматривается эффективность использования систем видео-
наблюдения и видеоаналитики для обеспечения безопасности на объектах
транспортной инфраструктуры (аэропорты) с учетом имеющихся в территори-
альных органах внутренних дел на транспорте технических средств, а также
технической и экономической целесообразности их применения.

Предназначено для курсантов, слушателей, профессорско-преподава-
тельского состава образовательных организаций системы МВД России, сотрудни-
ков территориальных органов МВД России на транспорте.

УДК 004: 351.749
ББК 67.401.133.12

ISBN 978-5-91776-225-8

© РИО Бел ЮИ МВД России
имени И.Д. Путилина, 2018

СОДЕРЖАНИЕ

Введение	4
1. Организация обеспечения безопасности объектов транспортной инфраструктуры (аэропортов) с использованием видеонаблюдения и видеоаналитики	6
1.1. Правовая основа использования систем видеонаблюдения и видеоаналитики в системе обеспечения безопасности аэропортов	6
1.2. Классификация и категорирование аэропортов как объектов транспортной инфраструктуры	13
1.3. Общие принципы построения систем видеонаблюдения	18
1.4. Видеоаналитика: понятие, основные модули, особенности применения	24
Контрольные вопросы	44
2. Технические средства и программное обеспечение, используемые в системах видеонаблюдения и видеоаналитики аэропортов	45
2.1. Элементы системы видеонаблюдения аэропорта: технические характеристики и особенности применения	45
2.2. Элементы системы видеоаналитики аэропорта: технические характеристики, программное обеспечение и особенности применения	58
Контрольные вопросы	68
Заключение	69
Библиографический список	70
Принятые сокращения	72

ВВЕДЕНИЕ

Аэропорты – с точки зрения обеспечения безопасности – одни из самых сложных объектов гражданской инфраструктуры. Вопрос обеспечения безопасности на воздушном транспорте является особенно острым и актуальным на современном этапе.

Современный комплекс сооружений аэропорта состоит не только из взлетно-посадочной полосы и здания аэровокзала, но и станций пассажирского транспорта (железнодорожного или автобусного), сложных автомобильных развязок и парковок, огромных комплексов технического обслуживания авиатехники и многокилометровых периметров, окружающих совокупность зданий и сооружений, называемых аэропортом. Поэтому и обеспечение безопасности аэропорта начинается не с прохождения предполетного досмотра и даже не с входа в здание аэровокзала, а намного раньше, еще на подъездах к нему.

В общем случае технические средства охраны объектов по функциональному назначению подразделяются на:

- извещатели охранные;
- приборы приемно-контрольные охранные;
- системы оповещения и шифроустройства;
- устройства систем передачи извещений (ретрансляторы, пульта централизованного наблюдения);
- интерфейсы сигнальные;
- источники электропитания для ТСО, систем контроля и управления доступом и систем охранных телевизионных;
- системы контроля и управления доступом;
- системы видеонаблюдения.

Одной из основных систем, обеспечивающих безопасность аэропорта, является система видеонаблюдения. Необходимо отметить, что современная система видеонаблюдения не только обеспечивает безопасность, но и помогает в целом управлять процессами, происходящими на объекте.

Аэропорт является большой и сложной системой для видеонаблюдения. Задачи видеомониторинга на крупных объектах требуют непрерывного контроля операторами сотен видеокамер, часть из которых должны быть поворотными. Решить задачи анализа изображения силами одних операторов невозможно. Поэтому для управления большим количеством видеокамер используются автоматизированные системы видеонаблюдения. Функционирование подобных систем невозможно без соответствующего программного обеспечения, которое получило общее название – видеоаналитика.

Автоматизированная система видеонаблюдения, совместно с программным обеспечением видеоаналитики, выявляет тревожные или подозрительные события без участия человека и выводит их на экран оператора в автоматическом режиме. При этом в последние годы наблюдается существенное улучшение качества работы техники и программного обеспечения с одновременным снижением их стоимости. Например, современные камеры высокого разрешения могут фиксировать объекты на расстоянии до двух километров. А внедрение системы ранжирования событий позволяет реагировать в первую очередь на наиболее важные события, не терпящие отлагательств. Модули видеоаналитики распознают дым или очаг пожара, драку, оставленный посторонний предмет, фиксируют появление нарушителя в запрещенной зоне. Система видеоаналитики может искать человека по цвету одежды, по скорости перемещения, позволяет анализировать траекторию движения в заданной зоне.

Аналитический обзор направлен на рассмотрение общих вопросов видеонаблюдения и видеоаналитики на объектах транспортной инфраструктуры. В первом разделе аналитического обзора устанавливаются основания использования видеонаблюдения и видеоаналитики в аэропортах. Также в первом разделе дано краткое описание видеонаблюдения и видеоаналитики и их основных элементов. Во втором разделе аналитического обзора дано обоснование технических решений при выборе типов видеокамер и модулей видеоаналитики с точки зрения решения ими необходимых задач на охраняемых объектах.

1. ОРГАНИЗАЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ (АЭРОПОРТОВ) С ИСПОЛЬЗОВАНИЕМ ВИДЕОНАБЛЮДЕНИЯ И ВИДЕОАНАЛИТИКИ

1.1. Правовая основа использования систем видеонаблюдения и видеоаналитики в системе обеспечения безопасности аэропортов

Внедрение систем обеспечения безопасности на объектах транспортной инфраструктуры на воздушном транспорте, в том числе видеонаблюдения и видеоаналитики, предусмотрено законодательными и нормативными правовыми актами. Основными из них являются:

1. Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности»¹ (далее – ФЗ «О транспортной безопасности»).
2. Постановление Правительства Российской Федерации от 23.01.2016 № 29².
3. Постановление Правительства Российской Федерации от 01.02.2011 № 42³.
4. Приказ Минтранса России от 21.02.2011 № 62⁴.
5. Приказ Минтранса России от 08.02.2011 № 40⁵.
6. Приказ Минтранса России от 28.11.2005 № 142⁶.

Рассмотрим требования к применению систем видеонаблюдения и видеоаналитики, установленные в указанных правовых актах.

¹ Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности» (ред. от 06.07.2016) // Собрание законодательства Российской Федерации. 2007. № 7. Ст. 837.

² Постановление Правительства РФ от 23.01.2016 № 29 «Об утверждении требований по обеспечению транспортной безопасности объектов транспортной инфраструктуры по видам транспорта на этапе их проектирования и строительства и требований по обеспечению транспортной безопасности объектов (зданий, строений, сооружений), не являющихся объектами транспортной инфраструктуры и расположенных на земельных участках, прилегающих к объектам транспортной инфраструктуры и отнесенных в соответствии с земельным законодательством Российской Федерации к охраняемым зонам земель транспорта, и о внесении изменений в Положение о составе разделов проектной документации и требованиях к их содержанию» // Собрание законодательства Российской Федерации. 2016. № 5. Ст. 698.

³ Постановление Правительства РФ от 01.02.2011 № 42 «Об утверждении Правил охраны аэропортов и объектов их инфраструктуры» (ред. от 17.12.2016) // Российская газета. 2011. № 25.

⁴ Приказ Минтранса России от 21.02.2011 № 62 «О Порядке установления количества категорий и критериев категорирования объектов транспортной инфраструктуры и транспортных средств компетентными органами в области обеспечения транспортной безопасности» (ред. от 10.10.2013) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2011. № 15.

⁵ Приказ Минтранса России от 08.02.2011 № 40 «Об утверждении Требований по обеспечению транспортной безопасности, учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств воздушного транспорта» (ред. от 10.10.2013) // Российская газета. 2011. № 54.

⁶ Приказ Минтранса России от 28.11.2005 № 142 «Об утверждении Федеральных авиационных правил "Требования авиационной безопасности к аэропортам"» (ред. от 24.05.2017) // Бюллетень нормативных актов федеральных органов исполнительной власти. № 4. 2006.

Статья 6 **Федерального закона Российской Федерации «О транспортной безопасности»** предусматривает, что объекты транспортной инфраструктуры и транспортные средства подлежат обязательному категорированию с учетом степени угрозы совершения акта незаконного вмешательства и его возможных последствий.

Понятие категорирования закреплено в п. 2 ст. 1 ФЗ «О транспортной безопасности»: категорирование объектов транспортной инфраструктуры и транспортных средств – отнесение их к определенным категориям с учетом степени угрозы совершения акта незаконного вмешательства и его возможных последствий.

В зависимости от категории объекта транспортной инфраструктуры к нему предъявляются различные требования по обеспечению безопасности, закрепленные в плане обеспечения транспортной безопасности объекта транспортной инфраструктуры. В соответствии с п. 10 ст. 9 ФЗ «О транспортной безопасности» план обеспечения транспортной безопасности аэропорта (аэродрома) является программой авиационной безопасности соответствующего аэропорта (аэродрома), предусмотренной международными стандартами Международной организации гражданской авиации в области защиты гражданской авиации от актов незаконного вмешательства, и разрабатывается с учетом требований, установленных международными договорами Российской Федерации, ФЗ «О транспортной безопасности», а также принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.

Пункт 8 статьи 12.2 ФЗ «О транспортной безопасности» установил, что для обеспечения безопасности применяются технические средства обеспечения транспортной безопасности – системы и средства сигнализации, контроля доступа, досмотра, *видеонаблюдения, аудио- и видеозаписи*, связи, оповещения, сбора, обработки, приема и передачи информации, предназначенные для использования на объектах транспортной инфраструктуры и транспортных средствах в целях обеспечения транспортной безопасности. Указанные технические средства подлежат обязательной сертификации. Требования к функциональным свойствам технических средств обеспечения транспортной безопасности и порядок их сертификации определяются Правительством РФ.

Таким образом, ФЗ «О транспортной безопасности» предусматривает, что на воздушном транспорте (в аэропортах) должны применяться для обеспечения безопасности средства видеонаблюдения и видеозаписи, прошедшие обязательную сертификацию.

Положения ФЗ «О транспортной безопасности» были развиты и конкретизированы в Постановлениях Правительства Российской Федерации, Приказах Минтранса России и государственных стандартах.

Постановление Правительства Российской Федерации от 23.01.2016 № 29 «Об утверждении требований по обеспечению транспортной безопасности объектов транспортной инфраструктуры по видам транспорта на этапе их проектирования и строительства и требований по обеспечению транспортной безопасности объектов (зданий, строений, сооружений), не являющихся объектами транспортной инфраструктуры и расположенных

на земельных участках, прилегающих к объектам транспортной инфраструктуры и отнесенных в соответствии с земельным законодательством Российской Федерации к охранным зонам земель транспорта, и о внесении изменений в Положение о составе разделов проектной документации и требованиях к их содержанию» определило требования по обеспечению транспортной безопасности аэропортов на этапе их проектирования и строительства.

В Постановлении Правительства Российской Федерации от 23.01.2016 № 29 установлено, что разрабатываемая проектная документация для строительства объекта транспортной инфраструктуры должна предусматривать проектные решения, направленные на оснащение объекта транспортной инфраструктуры техническими средствами обеспечения транспортной безопасности. К указанным средствам относятся, в том числе, системы видеонаблюдения и видеоаналитики.

Постановление Правительства Российской Федерации от 01.02.2011 № 42 «Об утверждении Правил охраны аэропортов и объектов их инфраструктуры» в пункте 6 установило, что в целях осуществления охраны периметра аэропорта устанавливается ограждение, а также организуются контрольно-пропускные пункты. Ограждение аэропорта оборудуется инженерно-техническими системами, обеспечивающими воспрепятствование несанкционированному проникновению лиц и транспортных средств на территорию аэропорта. Указанные инженерно-технические системы включают в свой состав системы видеонаблюдения и видеоаналитики.

Также в пункте 9 Постановления Правительства Российской Федерации от 01.02.2011 № 42 закреплено, что на территории международного аэропорта создаются непрерывно функционирующие посты (пункты) управления охраной аэропорта и объектов его инфраструктуры, оборудованные техническими средствами для сбора, обработки и хранения в электронном виде данных со всех инженерно-технических систем охраны, с автоматической передачей этих данных в режиме реального времени органам федеральной службы безопасности, Федеральной службе войск национальной гвардии Российской Федерации, а также Федеральной службе по надзору в сфере транспорта. Таким образом, все данные видеонаблюдения и видеоаналитики в международном аэропорте должны фиксироваться и передаваться в ФСБ и Росгвардию в реальном масштабе времени.

Приказ Минтранса России от 21.02.2011 № 62 «О Порядке установления количества категорий и критериев категорирования объектов транспортной инфраструктуры и транспортных средств компетентными органами в области обеспечения транспортной безопасности» закрепил, что критериями категорирования объектов транспортной инфраструктуры или транспортных средств являются:

п. 5.1. Степень угрозы совершения акта незаконного вмешательства в деятельность объектов транспортной инфраструктуры и/или транспортных средств применительно к отдельным видам транспорта, которая определяется на основании количественных показателей статистических данных (сведений) о совершенных и предотвращенных актах незаконного вмешательства на территории Российской Федерации (за исключением заведомо ложных сообще-

ний об угрозе совершения и/или совершении акта незаконного вмешательства), в том числе в отношении категорируемых объектов транспортной инфраструктуры и транспортных средств, за период последних 12-ти месяцев до момента категорирования;

п. 5.2. Возможные последствия совершения акта незаконного вмешательства в деятельность объектов транспортной инфраструктуры и/или транспортных средств применительно к отдельным видам транспорта, которые определяются на основании количественных показателей о возможных погибших или получивших вред здоровью людей, о возможном материальном ущербе.

Также Приказ Минтранса России от 21.02.2011 № 62 в Приложении 2 установил, что в зависимости от количественных показателей статистических данных (сведений) о совершенных и предотвращенных актах незаконного вмешательства (далее – АНВ) аэропортам могут присваиваться 5 категорий безопасности объекта в порядке убывания их значимости – первая, вторая, третья, четвертая, пятая – и закрепил критерии отнесения объектов транспортной безопасности к определенным категориям. По результатам категорирования объекту транспортной инфраструктуры и/или транспортному средству присваивается категория, соответствующая наивысшему количественному показателю любого из критериев категорирования.

Приказ Минтранса России от 08.02.2011 № 40 «Об утверждении Требований по обеспечению транспортной безопасности, учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств воздушного транспорта» предусматривает, что технические средства обеспечения транспортной безопасности (видеонаблюдение и видеоаналитика, а также хранение их результатов) должны обеспечивать:

1. Для объектов транспортной инфраструктуры всех категорий:

п. 5.2.4. круглосуточное непрерывное функционирование постов (пунктов) управления обеспечением транспортной безопасности объекта транспортной инфраструктуры или транспортного средства, а также накопление, обработку и хранение в электронном виде данных со всех технических средств обеспечения транспортной безопасности и передачу указанных данных в соответствии с утвержденными планами обеспечения транспортной безопасности;

п. 5.2.5. видеонаблюдение за действиями сил транспортной безопасности на КПП и постах (пунктах) управления обеспечением транспортной безопасности объекта транспортной инфраструктуры или транспортного средства.

2. Для объектов транспортной инфраструктуры первой категории:

п. 6.3.1. идентификацию физических лиц, являющихся объектами видеонаблюдения, на основании данных видеонаблюдения (далее – видеоидентификацию) на границах зоны транспортной безопасности и/или критических элементов объектов транспортной инфраструктуры (далее – ОТИ);

п. 6.3.2. обнаружение и распознавание характера событий, связанных с объектами видеонаблюдения, на основании данных видеонаблюдения и их обнаружение в произвольном месте и в произвольное время (далее – видеораспознавание) в перевозочном секторе зоны транспортной безопасности и на критических элементах ОТИ;

п. 6.3.3. обнаружение физических лиц и транспортных средств, являющихся объектами видеонаблюдения на основании данных видеонаблюдения в произвольном месте и в произвольное время (далее – видеообнаружение) в технологическом секторе зоны транспортной безопасности ОТИ;

п. 6.3.4. обнаружение физических лиц и транспортных средств, являющихся объектами видеонаблюдения, в заданном месте и в заданное время (далее – видеомониторинг) по периметру зоны транспортной безопасности и в зоне свободного доступа ОТИ;

п. 6.3.5. передачу видеоизображения в соответствии с порядком передачи данных с инженерно-технических систем в реальном времени;

п. 6.3.6. хранение в электронном виде данных со всех технических средств обеспечения транспортной безопасности в течение одного месяца;

п. 6.3.10. принятие решения о соответствии постоянного пропуска предъавителю с применением биометрических устройств на контрольно-пропускных пунктах (далее – КПП) на границах зоны транспортной безопасности и критических элементов ОТИ.

3. Для объектов транспортной инфраструктуры второй категории:

п. 10.5.1. видеоидентификацию объектов видеонаблюдения, перемещающихся на границах зоны транспортной безопасности и критических элементов объектов транспортной инфраструктуры;

п. 10.5.2. видеораспознавание объектов видеонаблюдения на критических элементах объектов транспортной инфраструктуры;

п. 10.5.3. видеообнаружение объектов видеонаблюдения на территории перевозочного сектора зоны транспортной безопасности;

п. 10.5.4. видеомониторинг объектов видеонаблюдения в границах технологического сектора зоны транспортной безопасности;

п. 10.5.5. передачу видеоизображения в соответствии с порядком передачи данных с инженерно-технических систем в реальном времени;

п. 10.5.6. хранение в электронном виде данных со всех технических средств обеспечения транспортной безопасности в течение 15 суток;

п. 10.5.10. принятие решения о соответствии пропуска предъавителя его владельцу с применением биометрических устройств или иным путем, обеспечивающим достоверное сличение идентифицирующих признаков на КПП на границах зоны транспортной безопасности и критических элементов ОТИ.

4. Для объектов транспортной инфраструктуры третьей категории:

п. 14.4.1. видеоидентификацию объектов видеонаблюдения, перемещающихся на границах зоны транспортной безопасности и критических элементов объектов транспортной инфраструктуры;

п. 14.4.2. видеообнаружение объектов видеонаблюдения на критических элементах объектов транспортной инфраструктуры;

п. 14.4.3. видеомониторинг объектов видеонаблюдения на территории перевозочного сектора зоны транспортной безопасности;

п. 14.4.4. возможность передачи видеоизображения в соответствии с порядком передачи данных с инженерно-технических систем в реальном времени;

п. 14.4.5. хранение в электронном виде данных со всех технических средств обеспечения транспортной безопасности в течение 10 суток.

5. *Для объектов транспортной инфраструктуры четвертой категории:*

п. 18.4.1. видеоидентификацию объектов видеонаблюдения, перемещающихся на границах зоны транспортной безопасности и критических элементов объектов транспортной инфраструктуры;

п. 18.4.2. видеомониторинг объектов видеонаблюдения в границах перевозочного сектора зоны транспортной безопасности, критических элементов объектов транспортной инфраструктуры;

п. 18.4.3. возможность передачи видеоизображения в соответствии с порядком передачи данных с инженерно-технических систем;

п. 18.4.4. хранение в электронном виде данных со всех технических средств обеспечения транспортной безопасности в течение 5 суток.

6. *Для объектов транспортной инфраструктуры пятой категории:*

п. 38.2.1. видеомониторинг объектов видеонаблюдения во время эксплуатации ОТИ в границах перевозочного сектора зоны транспортной безопасности ОТИ, критических элементов ОТИ;

п. 38.2.2. возможность передачи видеоизображения в соответствии с порядком передачи данных с инженерно-технических систем;

п. 38.2.3. хранение в электронной форме данных со всех технических средств обеспечения транспортной безопасности в течение 30 суток.

Можно констатировать, что система видеонаблюдения должна быть смонтирована во всех аэропортах, вне зависимости от категории. В аэропортах от 1 до 4 категории должна быть обеспечена видеоидентификация объектов видеонаблюдения, перемещающихся на границах зоны транспортной безопасности и критических элементов ОТИ. В аэропортах от 1 до 3 категории должно быть обеспечено видеообнаружение объектов видеонаблюдения на критических элементах ОТИ. В аэропортах 1 и 2 категории должно быть обеспечено видеораспознавание объектов видеонаблюдения на критических элементах ОТИ.

Таким образом, аэропорты 1 и 2 категории должны быть обеспечены системами видеоаналитики, которые позволяют осуществлять видеораспознавание в автоматическом режиме. Видеообнаружение и видеоидентификация может быть обеспечена силами обычного видеонаблюдения. Соответственно, в аэропортах 3-5 категорий может быть смонтирована только система видеонаблюдения, без видеоаналитики.

Приказ Минтранса России от 28.11.2005 № 142 «Об утверждении Федеральных авиационных правил «Требования авиационной безопасности к аэропортам» определил общие положения обеспечения безопасности в аэропортах.

В п. 17 приказа Минтранса России от 28.11.2005 № 142 установлено, что КПП аэропортов 1-3 категории должно быть оборудовано системой видеонаблюдения и видеозаписи. Это позволяет осуществлять видеообнаружение.

П. 23 приказа определил, что в ограждении территории аэропорта в качестве средства обеспечения безопасности могут быть использованы системы за-

щитной сигнализации, *системы видеонаблюдения и видеозаписи*, охранное освещение, а также иные инженерные и технические средства охраны».

П. 36 приказа, в частности, установил, что в аэропорту предусматриваются помещения (пункты досмотра), которые оборудуются стационарными техническими средствами досмотра (рентгенотелевизионным интроскопом, стационарным металлоискателем, портативными (ручными) металлоискателями, средствами обнаружения взрывчатых веществ), а также *системой видеонаблюдения и видеозаписи, информация которой сохраняется в течение 1 месяца*.

Таким образом, приказ Минтранса России от 08.02.2011 № 40 предусматривает хранение видеоданных от 5 до 30 дней, в зависимости от категории аэропорта. А приказ Минтранса России от 28.11.2005 № 142 более жестко определяет необходимость хранения видеозаписей в зоне досмотра в течение 30 суток.

Требования к оборудованию и программному обеспечению, обеспечивающему видеонаблюдение и видеоаналитику, установлены в следующих государственных стандартах и рекомендациях:

1. ГОСТ Р 51558-2014. «Национальный стандарт Российской Федерации. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний»: утв. и введен в действие Приказом Росстандарта от 22.10.2014 № 1371-ст.

2. ГОСТ Р 56461-2015. «Национальный стандарт Российской Федерации. Безопасность транспортная. Общие требования»: утв. и введен в действие Приказом Росстандарта от 15.06.2015 № 699-ст.

3. ГОСТ Р 56875-2016. «Национальный стандарт Российской Федерации. Информационные технологии системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий»: утв. и введен в действие Приказом Росстандарта от 26.02.2016 № 81-ст.

4. ГОСТ 31817.1.1-2012 (ИЕС 60839-1-1:1988). «Межгосударственный стандарт. Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения»: введен в действие Приказом Росстандарта от 22.11.2012 № 1034-ст.

5. ГОСТ Р 50776-95 (МЭК 60839-1-4:1989). «Государственный стандарт Российской Федерации. Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию»: принят и введен в действие Постановлением Госстандарта РФ от 22.05.1995 № 256 (ред. от 13.12.2011).

6. Р 78.36.018-2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»: утв. ГУВО МВД России 20.12.2011.

7. Р 78.36.002-2010 «Рекомендации. Выбор и применение систем охранных телевизионных»: утв. МВД России 07.05.2010.

8. Р 78.36.039-2014 «Рекомендации. Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения».

9. Р 78.36.029-2014 «Об оснащении ПЦО средствами аудио- и видеонаблюдения. Методические рекомендации».

1.2. Классификация и категорирование аэропортов как объектов транспортной инфраструктуры

Одним из основных условий, определяющих порядок использования видеонаблюдения и видеоаналитики на объекте транспортной инфраструктуры на воздушном транспорте (аэропорт) является категория и класс данного объекта.

Допуск аэродромов к эксплуатации осуществляется на основании решения комиссии, в которую входят представители федерального органа исполнительной власти, организации или объединения вида (рода войск) Вооруженных Сил Российской Федерации, в чьем оперативном управлении или хозяйственном ведении находится аэродром. Одним из направлений приемки объекта в эксплуатацию является охрана и оборона аэродрома.

По результатам работы комиссии составляется акт обследования аэродрома на соответствие требованиям норм годности к эксплуатации аэродромов. В случае выявления недостатков, препятствующих открытию аэродрома для эксплуатации воздушных судов, акт утверждается после устранения этих недостатков. В отдельных случаях аэродром допускается к эксплуатации при незначительном отступлении от требований норм годности к эксплуатации аэродромов, если они компенсируются введением мер, обеспечивающих эквивалентный уровень безопасности полетов. Для разработки предложений по обеспечению эквивалентного уровня безопасности полетов на аэродроме могут привлекаться компетентные в данной области научные организации.

Существует несколько видов классификации аэропортов.

В зависимости от вида поверхности взлетно-посадочных полос аэродромы делятся на следующие виды:

- с искусственным покрытием;
- грунтовые;
- снежные и ледовые;
- гидроаэродромы.

В зависимости от длины взлетно-посадочных полос аэродромы делятся на классы, определяемые длиной взлетно-посадочной полосы с искусственным покрытием в стандартных аэродромных условиях:

- класса А – аэродромы, имеющие взлетно-посадочную полосу длиной не менее 3200 метров;
- класса Б – не менее 2600 метров;
- класса В – не менее 1800 метров;
- класса Г – не менее 1300 метров;
- класса Д – не менее 1000 метров;
- класса Е – не менее 500 метров;
- неклассифицированные – аэродромы, имеющие взлетно-посадочную полосу длиной менее 500 метров и гидроаэродромы.

В соответствии с руководящими документами ИКАО (ICAO International Civil Aviation Organization – Международная организация гражданской авиации) классификация аэродромов осуществляется по кодовому обозначению. Кодовое обозначение состоит из двух элементов. Элемент 1 является номером, основанным на длине ВПП, а элемент 2 – буквой, соответствующей размаху крыла самолета и расстоянию между внешними колесами основного шасси в соответствии с табл. 1.

Таблица 1

Классификация аэродромов

Кодовый элемент 1		Кодовый элемент 2		
Кодовый номер	Длина взлетной полосы	Кодовая буква	Размах крыла	Расстояние между внешними колесами основного шасси
1	Менее 800 м	А	Менее 15 м	Менее 4,5 м
2	800 – 1200 м	В	15 – 24 м	4,5 – 6 м
3	1200 – 1800 м	С	24 – 36 м	6 – 9 м
4	1800 м и более	Д	36 – 52 м	9 – 14 м
		Е	52 – 60 м	9 – 14 м

Для целей проектирования, эксплуатации и сертификации аэропорты делятся на классы в зависимости от объемов и профиля выполняемых работ в соответствии с нормативными документами, регламентирующими проектирование, строительство, эксплуатацию и сертификацию аэропортов.

В зависимости от типа выполняемых перевозок аэропорты делятся на международные и для внутренних перевозок.

К международным относятся аэропорты, через которые разрешено в установленном порядке осуществлять международные авиационные перевозки и в которых обеспечивается соответствующий таможенный, пограничный и санитарно-карантинный контроль.

К аэропортам для внутренних перевозок относятся аэропорты, не имеющие разрешения на выполнение международных авиационных полетов, перевозки через которые, как правило, осуществляются в пределах Российской Федерации и без прохождения процедур таможенного, пограничного и санитарно-карантинного контроля, проводимого в международных аэропортах.

В зависимости от установленного статуса аэропорты делятся на аэропорты федерального, регионального (республиканского) значения и аэропорты местных воздушных линий.

К аэропортам федерального значения относятся аэропорты, составляющие главные узловые элементы национальной авиатранспортной системы Российской Федерации, обеспечивающие стабильное функционирование наиболее значимых межрегиональных (магистральных) и международных авиасвязей Российской Федерации. В состав аэропортов федерального значения включаются, как правило, аэропорты, годовой объем пассажирских перевозок через которые составляет не менее 500 тыс. человек, имеющие взлетно-посадочную полосу с ис-

кусственным покрытием и комплекс радионавигационного и светосигнального оборудования, позволяющие осуществлять полеты воздушных судов 1 и 2 класса или отнесенные к федеральным с учетом их социально-политического значения в системе государственного устройства Российской Федерации.

К аэропортам регионального значения (республиканского – в случае, если соответствующий аэропорт расположен в столице республики в составе Российской Федерации) относятся не являющиеся федеральными аэропорты, расположенные в административных центрах регионов и территориально-производственных комплексов, основной объем работ которых составляют межрегиональные магистральные авиаперевозки.

К аэропортам местных воздушных линий относятся аэропорты, в которых основной объем работ составляют внутрирегиональные авиатранспортные перевозки, а также полеты по применению авиации в народном хозяйстве.

В зависимости от объема воздушных перевозок аэропорты делятся на следующие классы, определяемые годовым объемом пассажирских перевозок, т.е. суммарным количеством всех прилетающих и вылетающих пассажиров, включая транзитных и трансфертных пассажиров:

- внеклассные – аэропорты с годовым объемом пассажиропотока более 15000 000 пассажиров;
- I класса – от 10000 000 до 15000 000 пассажиров;
- II класса – от 7000 000 до 10000 000 пассажиров;
- III класса – от 4000 000 до 7000 000 пассажиров;
- IV класса – от 1000 000 до 4000 000 пассажиров;
- V класса – от 100 000 до 1000 000 пассажиров;
- неклассифицированные – аэропорты с годовым объемом пассажиропотока менее 100 000 пассажиров.

В соответствии с Приказом Минтранса России от 21.02.2011 № 62⁷ *в зависимости от количественных показателей статистических данных (сведений) о совершенных и предотвращенных актах незаконного вмешательства на территории Российской Федерации (за исключением заведомо ложных сообщений об угрозе совершения и/или совершении акта незаконного вмешательства), за период последних 12 месяцев до момента категорирования присваиваются следующие категории:*

- применительно к ОТИ воздушного транспорта (категорирование объектов приведено в табл. 2).
- применительно к транспортным средствам (далее – ТС) воздушного транспорта (категорирование приведено в табл. 3).

⁷ Приказ Минтранса России от 21.02.2011 № 62 (ред. от 10.10.2013) «О Порядке установления количества категорий и критериев категорирования объектов транспортной инфраструктуры и транспортных средств компетентными органами в области обеспечения транспортной безопасности» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2011. № 15.

Таблица 2

Категорирование ОТИ воздушного транспорта

Значение категории ОТИ	Количество совершенных и/или предотвращенных АНВ на территории Российской Федерации, в том числе в отношении категорируемых объектов транспортной инфраструктуры
Первая	Два и более совершенных и/или предотвращенных АНВ в отношении категорируемого ОТИ и/или аналогичных объектов транспортной инфраструктуры на территории федерального округа Российской Федерации, в котором находится ОТИ, либо шесть и более в отношении аналогичных объектов транспортной инфраструктуры на территории Российской Федерации
Вторая	Один совершенный и/или предотвращенный АНВ в отношении категорируемого ОТИ или аналогичных объектов транспортной инфраструктуры на территории федерального округа Российской Федерации, в котором находится ОТИ, либо от трех до пяти в отношении аналогичных объектов транспортной инфраструктуры на территории других федеральных округов Российской Федерации
Третья	Два совершенных и/или предотвращенных АНВ в отношении аналогичных объектов транспортной инфраструктуры на территории других федеральных округов Российской Федерации
Четвертая	Один совершенный и/или предотвращенный АНВ в отношении аналогичных объектов транспортной инфраструктуры на территории других федеральных округов Российской Федерации
Пятая	Не зафиксировано совершенных и/или предотвращенных АНВ в отношении категорируемого ОТИ и/или аналогичных объектов транспортной инфраструктуры на территории субъектов Российской Федерации

Таблица 3

Категорирование ТС воздушного транспорта

Значение категории ТС	Количество совершенных и/или предотвращенных АНВ на территории Российской Федерации, в том числе в отношении категорируемых транспортных средств
Первая	Два и более совершенных и/или предотвращенных АНВ в отношении категорируемого ТС и/или транспортных средств воздушного транспорта в границах федерального округа Российской Федерации, в котором эксплуатируется и/или обслуживается ТС, а также в случае трех и более в отношении транспортных средств воздушного транспорта по маршруту полета категорируемого ТС в границах воздушного пространства Российской Федерации
Вторая	Один совершенный и/или предотвращенный АНВ в отношении категорируемого ТС и/или транспортных средств воздушного транспорта в границах федерального округа Российской Федерации, в котором эксплуатируется и/или обслуживается ТС, а также в случае двух в отношении транспортных средств воздушного транспорта по маршруту полета категориру-

	емого ТС в границах воздушного пространства Российской Федерации
Третья	Один совершенный и/или предотвращенный АНВ в отношении транспортных средств воздушного транспорта по маршруту полета категорируемого ТС в границах воздушного пространства Российской Федерации
Четвертая	Не зафиксировано совершенных и/или предотвращенных АНВ в отношении категорируемого ТС и/или транспортных средств воздушного транспорта в границах федерального округа Российской Федерации, в котором эксплуатируется и/или обслуживается ТС, а также в отношении транспортных средств воздушного транспорта по маршруту полета категорируемого ТС в границах воздушного пространства Российской Федерации

В зависимости от количественных показателей о возможных погибших или получивших вред здоровью людей ОТИ и ТС воздушного транспорта присваиваются категории, приведенные в табл. 4.

Таблица 4

Категорирование по количеству пострадавшего населения

Категория ОТИ и ТС	Возможное количество погибших или получивших вред здоровью людей, чел.
Первая	ОТИ – более 2000
	ТС – более 210
Вторая	ОТИ – от 500 до 2000
	ТС – от 120 до 210
Третья	ОТИ – от 100 до 500
	ТС – от 40 до 120
Четвертая	ОТИ – от 40 до 100
	ТС – до 40
Пятая	ОТИ – до 40

В зависимости от количественных показателей о возможном материальном ущербе и ущербе окружающей природной среде ОТИ и ТС воздушного транспорта присваиваются категории, представленные в табл. 5.

Таблица 5

Категорирование по количеству материального ущерба и ущерба окружающей природной среде

Категория ОТИ и ТС	Возможный материальный ущерб и ущерб окружающей природной среде, руб.
Первая	ОТИ – более 500 млн
	ТС – более 500 млн
Вторая	ОТИ – от 250 млн до 500 млн
	ТС – от 250 млн до 500 млн
Третья	ОТИ – от 10 млн до 250 млн
	ТС – от 10 млн до 250 млн
Четвертая	ОТИ – менее 10 млн
	ТС – менее 10 млн
Пятая	ОТИ – менее 10 млн

Также необходимо обратить внимание на тот факт, что в зависимости от категории аэропорта его охрана осуществляется различными субъектами. При этом охрана аэропортов третьей, четвертой и пятой категорий охраняемыми предприятиями (службами авиационной безопасности) осуществляется, как правило, самостоятельно.

Соответственно, работу с системами видеонаблюдения и видеоаналитики осуществляют сотрудники служб авиационной безопасности. Они же и осуществляют реагирования на нештатные ситуации. Аэропорты первой и второй категории в соответствии с Перечнем, утвержденным Распоряжением Правительства Российской Федерации от 15 мая 2017 г. № 928-р «Об утверждении перечня объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации»⁸, охраняются Росгвардией.

Однако реагирование на нештатные ситуации осуществляется ими совместно с сотрудниками Росгвардии. Сотрудники органов внутренних дел непосредственно в охране, видеонаблюдении и работе с видеоаналитикой не участвуют и привлекаются при выявлении преступлений или правонарушений.

Рассмотрев классификацию аэропортов, перейдем к рассмотрению понятия видеонаблюдения и техническим средствам, которые его обеспечивают.

1.3. Общие принципы построения систем видеонаблюдения

В современном мире системы видеонаблюдения – это надежный способ обеспечения безопасности людей и объектов, а также сохранности материальных ценностей. Видеонаблюдение используется как для бизнеса, так и в личном пространстве, будь то квартира, загородный дом или парковочное место. Сферы использования систем видеонаблюдения неограниченны, а их аппаратные и программные возможности непрерывно совершенствуются, делая охранное наблюдение все более простым, удобным и доступным инструментом.

Одним из основных направлений использования видеонаблюдения является обеспечение безопасности на объектах транспорта и транспортной инфраструктуры. Необходимо отметить, что активное использование систем видеонаблюдения, в том числе с выводом изображения в дежурные части, является одним из основных способов профилактики и раскрытия преступлений на транспорте.

Видеокамеры устанавливаются как внутри вокзалов и станций, в парках подвижного железнодорожного состава, на мостах и в тоннелях. Кроме того, видеокамерами должны контролироваться подходы к объектам транспортной инфраструктуры извне, особенно в местах большого потока пассажиров.

⁸ Распоряжение Правительства Российской Федерации от 15.05.2017 № 928-р «О перечне объектов, подлежащих обязательной охране войсками национальной гвардии» // Собрание законодательства Российской Федерации. 2017. № 21. Ст. 3065.

Видеонаблюдение – это процесс, осуществляемый с применением оптико-электронных устройств, предназначенных для визуального контроля или автоматического анализа изображений.

Система видеонаблюдения – это телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений с охраняемого объекта в целях обеспечения антикриминальной защиты.

Как мы рассмотрели в первом параграфе, системой видеонаблюдения должен быть оборудован любой объект транспортной инфраструктуры на воздушном транспорте, вне зависимости от категории. Чем выше категория (от пятой к первой), тем более функциональной и сложной должна быть система видеонаблюдения. Причем, она включает в себя не только замкнутую систему охранного телевидения, но и комплект оборудования для передачи видеoinформации по различным каналам связи, (как проводным, так и с использованием радиоканалов). В результате установки в аэропорте технических средств и программного обеспечения видеонаблюдения должны быть достигнуты следующие результаты:

1. Создана локальная система видеонаблюдения с выводом информации на пункт централизованной охраны (далее – ПЦО) (см. рис. 1.1).
2. Реализована возможность удаленного мониторинга обстановки на ПЦО с передачей видеoinформации вышестоящему звену управления.
3. Реализована возможность верификации тревог на охраняемых объектах с контролем действия групп задержания на этих объектах.
4. Обеспечена возможность передачи видеoinформации посредством сетевых технологий на значительное расстояние.
5. Реализована возможность удаленного доступа к архиву аудио- и видеoinформации.



Рис. 1.1. Пункт видеонаблюдения (ситуационный центр) аэропорт города Измир (Турция).

При этом создаваемая система видеонаблюдения должна быть адаптивной и позволять:

- при отсутствии физических линий связи (оптоволоконных или проводных линий) осуществлять передачу видеoinформации по радиоканалу большого радиуса действия стандарта «4G» и «Wi-Fi»;
- осуществлять автоматическую настройку параметров изображений;
- управлять удаленными регистраторами, в том числе по протоколу http;
- объединять несколько отдельно стоящих объектов охраны в единый комплекс за счет использования радиоканалов ближнего радиуса действий.

Архитектура системы видеонаблюдения должна быть организована по модульному принципу, что впоследствии позволит объединить системы видеонаблюдения в глобальную систему видеонаблюдения.

Существует несколько общих проблем при построении систем видеонаблюдения. К ним относятся пропускная способность канала передачи данных и выбор алгоритма компрессии, фокусное расстояние объектива камер, использование видеокамер в условиях ограниченной видимости.

В системах видеонаблюдения одним из самых «узких» мест являются *каналы передачи видеоданных*, поэтому следует обратить на это особое внимание.

При расчете пропускной возможности канала связи для одного видеоканала без использования компрессии видеосигнала учитываются следующие исходные данные:

- разрешение – ширина спектра, для видеосигнала стандартного разрешения верхняя граница спектра составляет 6 МГц, а для видеосигнала высокой четкости – 30 МГц;
- количество кадров – не менее 25 кадров/сек;
- разрядность аналого-цифрового преобразователя – не менее 10 бит.

В общем случае, необходимая пропускная способность канала связи без использования того или иного вида компрессии – 3 Гб/сек. Стандартные компьютерные сети обычно не позволяют передавать информацию со скоростью больше 1 Гб/с.

Следовательно, для эффективной работы системы видеонаблюдения необходимо использовать тот или иной *вид компрессии видеосигнала*. Основные виды компрессии делятся на алгоритмы с покадровым сжатием (каждый кадр сжимается независимо друг от друга) и алгоритмы с межкадровым сжатием (сжатие происходит с учетом изменения информации в предыдущих кадрах). Алгоритмы с межкадровым сжатием позволяют при меньшей пропускной способности канала связи обеспечить заданное качество изображения.

В стандартах межкадровых алгоритмов компрессии (MPEG-2/4, H.264), наиболее часто используемых в охранном телевидении, зафиксированы требования к структуре сжатых данных. При этом способ вычисления отдельных параметров (вектор смещения движущихся объектов в промежуточных кадрах) определяется разработчиками конкретной реализации алгоритма. Поэтому качество реализации алгоритмов межкадровой компрессии в системах видеонаблюдения

разных производителей может существенно различаться. Это отражается на качестве картинки, а также на объеме потока компрессированных данных.

Следует отметить, что объем трафика при межкадровом алгоритме компрессии заметно меньше, чем при сжатии данных покадровыми кодеками. То же самое касается и размера архива видеоданных.

При межкадровом алгоритме сжатия производные кадры получаются искусственным способом, а именно, путем восстановления движущихся объектов предыдущего (или предыдущего и последующего) кадра по векторам смещения. Таким образом, в случае необходимости разбора инцидента, зафиксированного системой видеонаблюдения, возможно пригодных для анализа записи и идентификации объектов будет всего 1-2 опорных кадра (либо не будет). Обычно опорные кадры идут с интервалом 1-2 с, а промежутки между ними заполняются производными кадрами, не пригодными для анализа. В то же время у записи, сделанной системой видеонаблюдения с покадровым сжатием, каждый кадр представляет собой отдельный снимок и может быть использован для анализа.

Частота следования опорных кадров в межкадровых кодеках является регулируемой величиной. Однако при увеличении частоты следования опорных кадров до величины, близкой к покадровым кодекам, объем сетевого трафика (архива данных) возрастает и становится выше, чем у покадровых кодеков. Кроме того, покадровые кодеки имеют свойство, которое можно удачно использовать для масштабирования видеопотока и оптимизации сетевого трафика. Для проведения криминалистических экспертиз принимаются только кадры покадровых алгоритмов сжатия или опорные кадры межкадровых алгоритмов.

Таким образом, для задач, решаемых профессиональными охранными системами видеонаблюдения на крупных и средних объектах, более применимы системы видеонаблюдения с покадровыми алгоритмами компрессии. В случае небольших объектов, где не слишком важна документальность записей, а также нет жестких требований к качеству изображения, используют межкадровые кодеки.

Необходимая пропускная способность сильно зависит от выбранного алгоритма компрессии и степени динамического изменения изображения, уровня освещенности объекта наблюдения (от соотношения сигнал/шум), причем шум воспринимается алгоритмом компрессии как постоянное изменение, что снижает эффективность компрессии.

Выбор *фокусного расстояния объектива камер* видеонаблюдения еще одно из важных условий при построении системы видеонаблюдения.

При выборе фокусного расстояния объектива рекомендуется воспользоваться различными программами для расчета углов зрения и размеров изображения. Такими же важными характеристиками являются угол зрения по горизонту и расстояние до объекта наблюдения, наличие освещения.

При работе охранных телевизионных систем большое значение имеет возможность *обнаружения объектов наблюдения в условиях ограниченной видимости*. Часто климатические условия существенно ограничивают уровень освещенности наблюдаемых объектов. В то же время иногда, по тактическим соображениям, необходимо скрыть сам факт видеонаблюдения. Использование

инфракрасной подсветки ближнего диапазона существенно не влияет на ситуацию, поскольку она достаточно уверенно регистрируется стандартными видеокамерами, электронно-оптическими приборами и наблюдается даже в стандартный оптический прицел. Иногда подсветку объекта наблюдения не удается реализовать по техническим или экономическим соображениям. Не менее важно обеспечить работоспособность охранных телевизионных систем при воздействии внешних разрушающих воздействий.

Для наблюдения за объектами в условиях недостаточной освещенности могут использоваться:

- видеокамеры повышенной чувствительности;
- видеокамеры с суммированием по соседним пикселям и/или по кадрам;
- «противотуманные» видеокамеры;
- видеокамеры с электронным умножением (EM-CCD-камеры);
- электронно-оптические преобразователи;
- стробируемые электронно-оптические преобразователи;
- тепловизоры;
- приемники терагерцового диапазона (миллиметрового диапазона);
- комбинация обзорной РЛС с видеокамерой или тепловизором.

Более подробно о подобных программных продуктах изложено в статье А.В. Котельникова «Программные средства, предназначенные для расчетов параметров систем охранного телевидения»⁹. В данной статье приводятся и анализируются различные программы, поэтому есть возможность для широкого выбора.

Таким образом, при построении системы видеонаблюдения необходимо учитывать следующие общие требования:

1. Количество и качество видеокамер должно соответствовать нормам и сочетаться с показателями другого оборудования (емкость видеорегистратора, пропускная способность канала передачи данных, алгоритм компрессии, фокусное расстояние объектива камер).

2. Видеокамеры должны максимально перекрывать подходы друг к другу (направление съемки – встречное, т.е. видеокамеры смотрят друг на друга).

3. Место прохода сотрудников и посетителей обязательно контролируется видеокамерой, имеющей соответствующий угол зрения, для получения максимально большой информативности о входящих в здание людях.

4. Комната операторов ПЦО оборудована видеокамерой.

5. Входные двери в комнаты ПЦО оборудованы видеодомофонами.

6. Видеопоток просматривается оператором (локальный видеорегистратор) и дублируется в комнате начальника ПЦО (удаленный видеорегистратор).

7. Категория кабеля локальной сети – не ниже 5.

⁹ Котельников А.В. Программные средства, предназначенные для расчетов параметров систем охранного телевидения // Научно-технический портал МВД России. 2014. № 1(9).

Поскольку видеокамеры установлены на значительном расстоянии от помещений операторов видеонаблюдения и приоритет отдается качеству видеоизображения, то основные технические решения, в случае использования для работы с IP-камерами должны предусматривать:

- передачу видеоизображения в цифровом виде (при этом повышается помехоустойчивость линии передачи видеоинформации и отсутствуют искажения на этапах повторной ретрансляции данных);
- передачу видеоинформации (для аэропортов 1-3 категорий) в «реальном масштабе времени»;
- минимальную скорость записи не ниже четырех-шести кадров в секунду, а канал прямого видеонаблюдения должен обеспечивать скорость записи не менее 25 кадров в секунду. Для видеонаблюдения используется не менее двух видеомониторов (лучше всего четыре-шесть мониторов);
- в зависимости от приоритета и задач при видеонаблюдении необходимо использовать как купольные камеры, так и стационарные видеокамеры. Ряд камер необходимо оснастить объективом с трансфокатором, обеспечивающим десятикратное увеличение;
- все видеокамеры, устанавливаемые снаружи здания, должны быть помещены в термокожухи, а объективы оснащены авторегулируемой диафрагмой. Стационарные видеокамеры должны быть оборудованы объективом, позволяющим в ручном режиме изменять фокусное расстояние, а значит и угол зрения, от 3 до 10 раз (варифокальные объективы).

Отдельно необходимо обратить внимание на то, что одной из типичных ошибок при проектировании системы видеонаблюдения в аэропорту является отсутствие запаса по избыточности, что в дальнейшем ограничивает возможность быстрого расширения и модернизации системы видеонаблюдения.

Подводя итог рассмотрению общих принципов организации видеонаблюдения на объекте транспортной инфраструктуры, можно констатировать, что выполнение перечисленных выше требований позволит выполнить все положения нормативных актов по использованию видеонаблюдения в аэропортах. Кроме того, необходимо отметить, что система видеонаблюдения, как мы отмечали выше, не является самостоятельной, а работает в комплексе с другими системами обеспечения функционирования и безопасности аэропорта (см. рис. 1.2).



Рис. 1.2. Использование видеонаблюдения в Центре управления аэропортом «Шереметьево».

Рассмотрев общие вопросы функционирования систем видеонаблюдения в аэропорте, переходим к рассмотрению понятия и особенностей применения систем видеоаналитики на аэропортовых комплексах.

1.4. Видеоаналитика: понятие, основные модули, особенности применения

Использование современных цифровых технологий в организации видеонаблюдения позволяет существенно повысить его качество, а системы обеспечения безопасности становятся интеллектуальными. К системе видеонаблюдения можно подключить дополнительные модули, наделенные интеллектом, что позволит в разы увеличить возможности комплекса охранного телевидения. Такое интеллектуальное видеонаблюдение называется видеоаналитикой.

***Видеоаналитика** – это аппаратно-программное обеспечение или технология, использующая методы компьютерного зрения для автоматизированного сбора данных на основании анализа потокового видео (видеоанализа).*

В основу программного обеспечения видеоаналитики положен комплекс алгоритмов машинного зрения, позволяющих вести видеонаблюдение без прямого участия человека¹⁰. Кроме машинного зрения, видеоаналитика опирается на алгоритмы обработки изображения и распознавания образов, позволяющие анализировать видео без прямого участия человека.

¹⁰ Видеоаналитика. Материал из свободной энциклопедии Википедия. URL: <https://ru.wikipedia.org/wiki> (дата обращения: 20.08.2017).

Алгоритмы видеоаналитики могут быть интегрированы в различные системы, но чаще всего используются в составе интеллектуальных систем видеонаблюдения (ССТV, охранного телевидения) и других сферах безопасности.

Комплекс видеоаналитики состоит из двух частей¹¹. Первая – часть аппаратная. Она включает в себя видеосистему и специальные технические устройства, обеспечивающие ее функционирование. Вторая часть – программная. Она включает в себя специализированные информационные технологии, которые позволяют в собранной информации быстро ориентироваться.

Видеоаналитика бывает двух уровней. *Первый уровень видеоаналитики* – это обычный детектор движения, который отслеживает выделенную оператором зону, определяет нарушения, подает сигнал оператору и записывает видеосъемку нарушений в архив. Оператор впоследствии может просмотреть архив и обратиться напрямую к видеозаписи, которая содержит именно нарушение установленных ограничений. При этом детектор движения не обязательно должен быть встроен в камеру. Возможна установка специализированного программного обеспечения на сервер и использование программного детектора движения. Один детектор способен заменить сразу несколько операторов видеонаблюдения. А уже в 2000-е годы начали появляться первые системы видеоаналитики, способные распознавать объекты и события в кадре.

Причем сам оператор видеоаналитики не должен обладать специальными знаниями и навыками. Достаточно обладать навыками работы с архивом видеозаписей, выбрать события соответствующего временного интервала и записать в электронный журнал результаты проверки. При работе оператора с видеоаналитикой в области безопасности оператор постоянно присутствует и имеет возможность отследить нарушение в реальном масштабе времени, пресечь нарушение или предотвратить его.

Второй уровень видеоаналитики – «умные» детекторы, подразумевает предварительную обработку данных аналитическими детекторами движения, т.е. поступающая с них информация уже имеет определенное назначение и может вызывать заданные сценарии.

Аналитические детекторы обладают следующими возможностями:

1. Детекторы работают не с активностью в заданных зонах, а с объектами, обладающими определенными характеристиками, которые сами детекторы вычисляют. К таким характеристикам могут относиться: вектор движения (направление и кратковременная скорость), размеры, история (путь или трек объекта), тип объекта (человек или группа людей, транспортное средство).

2. Тревоги задаются уже по нарушениям объектами характера их движения в заданных областях, т.е. понятие зоны здесь аналогично базовой видеоаналитике. Часто еще встречается понятие «границы» – виртуальной линии, пересечение которой в том или ином направлении (и характеристиках объекта) будет вызывать тревогу или может просто считать объекты.

¹¹ Особенности использования информационных технологий в органах внутренних дел на транспорте: учебное пособие / И.Ф. Амельчаков, П.Н. Жукова, А.Н. Прокопенко [и др.]. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2016. – 118 с.

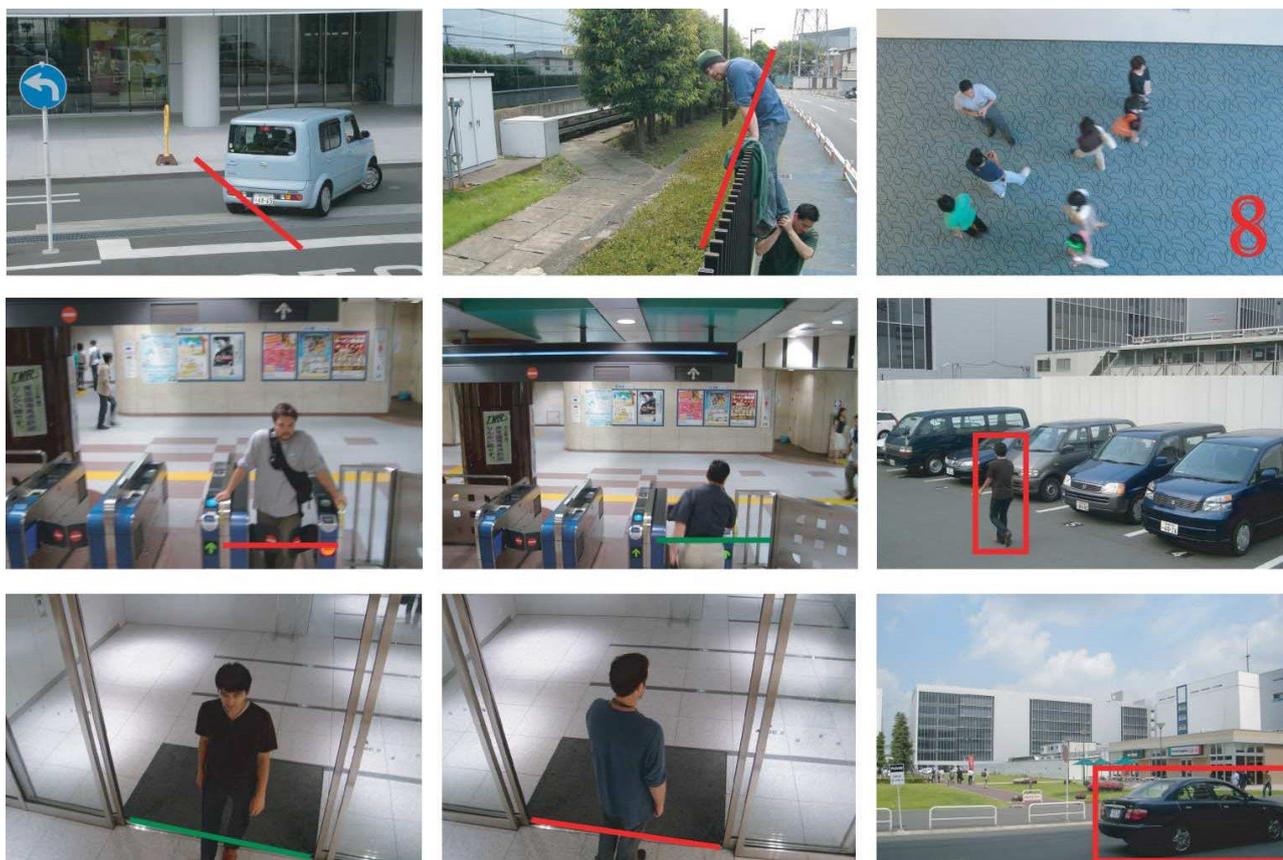


Рис. 1.3. Видеоаналитика в транспортной системе.

В зависимости от целей, видеоаналитика может реализовать как одну, так и несколько базовых функций. **Основными базовыми функциями «умной» видеоаналитики являются следующие:**

Обнаружение объектов. Как правило, обнаружение объектов в поле зрения камеры производится при помощи видеодетекторов движения. Основное отличие видеоаналитики от инфракрасных датчиков движения состоит в возможности выделения и независимом анализе сразу нескольких объектов. Если движение не является достаточным признаком для выделения объекта в кадре, то обнаружение может производиться при помощи шаблонов. Например, обнаружение лиц людей, номерных знаков автомобилей или обнаружение малопо- движных морских целей.

Слежение за объектами. Алгоритмы слежения (сопровождения) позволяют получить частную траекторию движения объекта как в поле зрения одной камеры, так и обобщенную траекторию по данным сразу нескольких камер. Слежение необходимо, чтобы проанализировать поведение объекта по его траектории, например, определить движение человека против потока или движение с повышенной скоростью. Кроме этого, слежение необходимо для исключения повторных срабатываний систем видеоаналитики на одни и те же объекты. Профессиональные системы работают по правилу «один тревожный объект – одно срабатывание» для достижения высокой продуктивности оператора.

Идентификация объектов. Идентификация объектов является наиболее сложным компонентом систем видеоаналитики. Современные системы позволяют идентифицировать людей по биометрическим признакам лица или транспортные средства – по номерным знакам (см. рис. 1.4). Идентификация может быть реализована при помощи дополнительных средств за рамками видеоаналитики: на основе отпечатков пальцев, банковской карты, билета, пропуска или идентификатора мобильного устройства.



Рис. 1.4. Распознавание автомобильного номера.

Обнаружение (распознавание) ситуаций. Видеоаналитика позволяет не только выделять объекты из потокового видео, но и распознавать тревожные ситуации на основе анализа поведения данного объекта, что не дает сделать обычная система видеонаблюдения. Также ситуационная видеоаналитика может автоматически детектировать пересечение сигнальной линии, падение людей, запрещенную парковку и возникновение пожара.

Классификация объектов. Некоторые системы видеоаналитики классифицируют объекты для фильтрации оперативных уведомлений или результатов поиска. **Классификатор объектов** автоматически дифференцирует объекты на 3 группы: человек, автомобиль и группа людей, рассчитывая при этом вероятность распознавания класса объекта (см. рис. 1.5). Помимо автоматизации и оптимизации работы оператора охранного пункта, классификатор позволяет решать такие задачи, как поиск в видеоархиве или задание правил оперативного реагирования на объекты конкретного класса. При этом важно, что признаки объекта вычисляются в реальных координатах, а не координатах изображения.

Принцип работы классификатора объектов:

- в кадре появляется объект, который обнаруживается видеоаналитикой;
- по мере движения объекта подсчитываются его размеры, скорость и форма;
- по форме объекта модуль слежения создает его маску;
- модуль анализирует кадр видео и маску, после чего определяет класс объекта.

Таким образом, в зависимости от целей видеоаналитика может реализовать как одну, так и несколько базовых функций: обнаружение объектов; слежение за объектами; идентификация объектов; обнаружение (распознавание) ситуаций.



Рис. 1.5. Работа типового классификатора объектов.

Видеоаналитика позволяет не только выделять объекты из потокового видео, но и распознавать тревожные ситуации на основе анализа поведения данного объекта, что не дает сделать обычная система видеонаблюдения. Также ситуационная видеоаналитика может автоматически детектировать пересечение сигнальной линии, падение людей, запрещенную парковку и возникновение пожара.

В результате работы видеоаналитики с «умными» детекторами формируются структуры данных, которые описывают содержание каждого кадра видеопоследовательности. Такие данные называются метаданными и содержат такую информацию, как местоположение и идентификаторы объектов (как правило, в виде тревожной рамки), траекторию и скорость движения объектов, данные о разделении или слиянии объектов, данные о возникновении и окончании тревожной ситуации. Оператор видит данную информацию в реальном масштабе времени и имеет возможность отреагировать на нарушения. Одновременно указанная информация записывается в архив.

«Умная» видеоаналитика обладает расширенными функциями, которые позволяют:

- прогнозировать поведение объекта или возникновение ситуаций (например, образование очереди на платформе метро или на кассе с учетом числа зашедших пассажиров);
- осуществлять интеллектуальное сжатие видеоконтента с учетом интереса потребителя (например, система передает только видео, содержащие тревожные ситуации);
- производить ранжирование (определение приоритета) событий видеоаналитики;
- формировать производные видеоданных (интегральный кадр, тайм-лапс), удалять персональные данные из видеоряда, например, при помощи детектора лиц и номерных знаков.

Основные виды и модули видеоаналитики

Ситуационная видеоаналитика применяется для распознавания тревожных ситуаций, связанных с поведением людей или с движением транспортных средств. Ситуационная видеоаналитика может работать на основе правил, заданных пользователем (например, запрещенная парковка перед пешеходным мостом на перрон), или на основе накопленной статистики (например, обнаружение на привокзальной площади в два раза больше людей, чем обычно в это время суток и в этот день недели).

В случае возникновения тревожной ситуации, видео с одной или нескольких камер автоматически отображается на мониторе службы безопасности, подается звуковой сигнал и действие оператора заносится в протокол.

Правила на основе **сигнальной линии** подразумевают задание линии, при пересечении которой в одном или обоих направлениях формируются следующие события:

- пересечение линии,
- парный проход (движение в хвосте),
- проход без пропуска/билета,
- движение против потока,
- проход на территорию слишком большого числа людей.

Сигнальная линия вдоль платформы метро или вокзала позволяет сформировать тревожное сообщение в случае падения человека на рельсы (см. рис. 1.6). При этом видеоаналитика не будет реагировать на движение поездов и перемещения пассажиров на платформе.



Рис. 1.6. Пересечение сигнальной линии.

Сигнальная линия вдоль забора позволяет зафиксировать момент тревоги в случае перелазу человека через ограждение (см. рис. 1.7).



Рис. 1.7. Обнаружение преодоления ограждения.

Правила на основе **сигнальной зоны** предполагают задание на видео многоугольника произвольной формы, на границе и внутри которого возможны вход в зону; выход из зоны; остановка; праздничное поведение; быстрое движение (бег); перемещение в определенном направлении; скопление людей; оставленный/исчезнувший предмет.

Детектор остановки объекта в зоне сигнализирует о неправильной парковке автомобиля на проезжей части или в пешеходной зоне, но в то же время не реагирует на проезжающие автомобили (см. рис. 1.8).

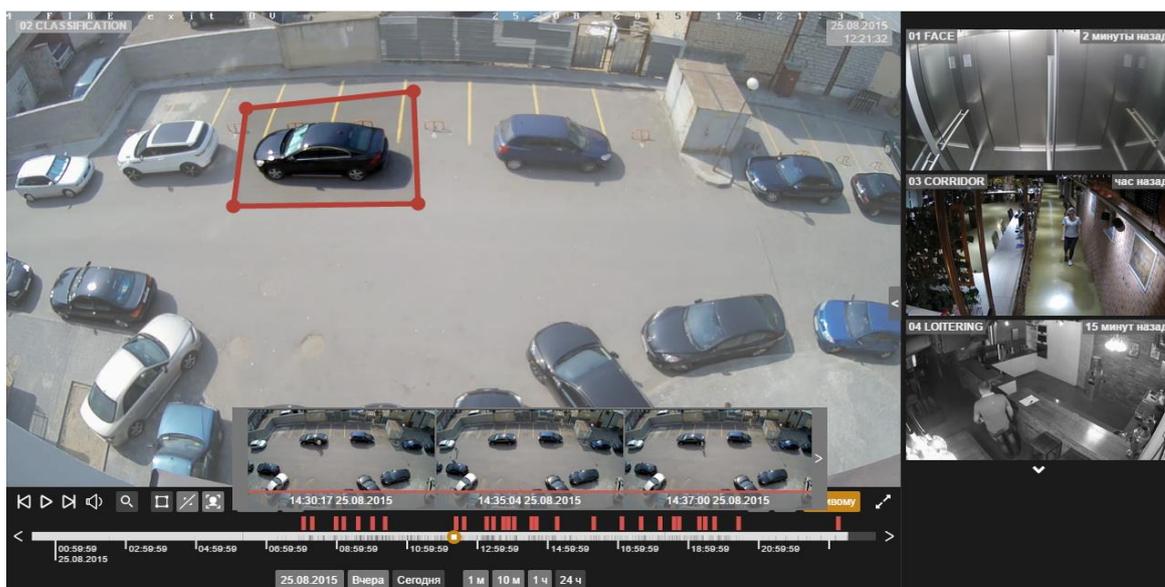


Рис. 1.8. Неправильная парковка в сигнальной зоне.

Детектор остановки объекта в зоне сигнализирует об остановке человека в неполюженном месте, но в то же время не реагирует на людей, просто идущих мимо (см. рис. 1.9).



Рис. 1.9. Обнаружение остановки человека возле охраняемого объекта.

Детектор быстрого движения сигнализирует только о перемещении объектов со скоростью, превышающей заранее заданное значение (см. рис. 1.10). Примером выступает человек, бегущий мимо охраняемого объекта.



Рис. 1.10. Обнаружение превышения скорости (бегающий человек).

Детектор перемещения в определенном направлении сигнализирует о движении объектов в неестественном направлении (см. рис. 1.11 (а) и (б)). Примером выступает человек, который начал забираться на лестницу дома, вместо того, чтобы передвигаться в горизонтальном направлении. Другим примером может выступать движение человека навстречу основному потоку людей.



Рис. 1.11 (а). Обнаружение перемещения в определенном направлении



Рис. 1.11 (б). Обнаружение движения в определенном направлении.

Детектор скопления людей предназначен для предупреждения правонарушений и массовых беспорядков на наблюдаемой территории. Детектор может быть использован как на улице и площадях, так и внутри помещений: метро, вокзалах, торговых и торгово-развлекательных центрах (см. рис. 1.12). Детектор скопления срабатывает при превышении заданного порога количества людей в наблюдаемой зоне. В купольных потолочных камерах распознавание скоплений людей осуществляется при помощи *модуля подсчета людей*.



Рис. 1.12. Использование детектора скопления людей.

Детектор активности предназначен для контроля присутствия персонала (операторов, дежурных, кассиров, охранников) на служебном месте. Детектор определяет состояние контролируемого персонала в заданной зоне: активен или пассивен.

Активность персонала определяется по принципу его подвижности. Если персонал отсутствует на месте или он малоподвижен (спит, читает книгу), то система идентифицирует его как отсутствующего (см. рис. 1.13).

Детектор персонала может решать следующие задачи:

- определение активности персонала;
- определение времени, которое оператор проводит на своем рабочем месте;
- уведомление, если оператор покинул свое рабочее место;
- уведомление о смене персонала на рабочем месте.

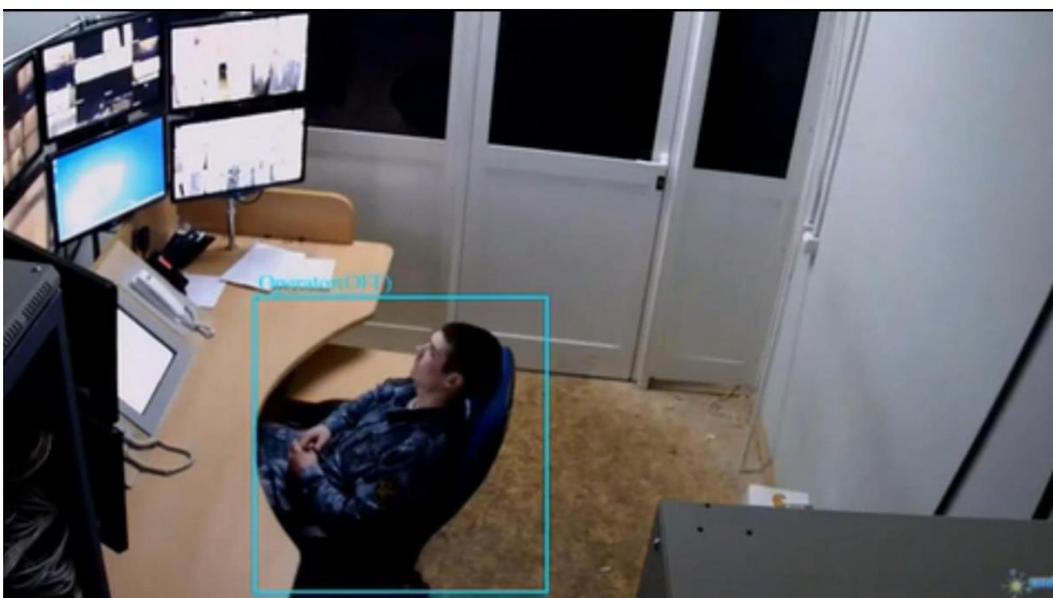


Рис. 1.13. Использование детектора персонала.

Детектор праздношатания опирается на современный алгоритм обнаружения и сопровождения объектов. Алгоритм устойчиво работает даже в условиях взаимного перекрытия этих объектов. В рамках работы охранных систем детектор является надежным инструментом для контроля лиц, передвигающихся на территории объекта.

Возможна настройка следующих параметров детектора праздношатания:

- зона правила (в виде многоугольника);
- время пребывания в зоне (в секундах).

При входе человека в зону срабатывает счетчик времени. При нахождении человека в зоне свыше указанного времени формируется событие «праздношатание» (см. рис. 1.14 (а), 1.14 (б)).



Рис. 1.14 (а). Использование детектора праздношатания.

Детектор праздношатания может быть использован для автоматического распознавания следующих ситуаций:

- человек задерживается перед подъездом или внутри подъезда;
- человек устанавливает взрывное устройство на железнодорожном полотне;
- человек занимается несанкционированной фото- или видеосъемкой;
- человек делает надписи (граффити) на стене.



Рис. 1.14 (а). Использование детектора праздношатания.

Детектор оставленных предметов (бесхозных или забытых вещей) предназначен для распознавания ситуаций, связанных с появлением в зоне наблюдения предметов, потенциально угрожающих безопасности, например, взрывного устройства.

Обнаружение оставленного предмета в местах массового скопления людей является сложной научно-технической задачей, которая на текущий момент полностью не решена ни одним из производителей систем видеоаналитики.

Тревожный сигнал формируется при условии выполнения трех правил:

- человек входит в зону наблюдения;
- рядом с человеком появляется неподвижный объект;
- человек выходит из зоны наблюдения.

Проверка трех условий позволяет снизить частоту ложных срабатываний детектора забытых предметов. Этот же алгоритм используется для обнаружения пропажи предметов (предмет исчезает из зоны при выходе оттуда человека). Возможно детектирование оставленных предметов заданного размера, как, например, остановившийся в кадре автомобиль. Обнаружение владельца оставленного предмета осуществляется путем анализа кадров, связанных с тревожным событием, в момент появления и в момент ухода человека.

Детектор оставленных предметов интегрируется с системой сопровождения объектов и регистрирует оставленные предметы с низкой частотой ложных срабатываний благодаря множеству критериев проверки гипотезы. Детектор встраивается непосредственно в камеру или видеозаписывающее устройство, что позволяет существенно снизить нагрузку на каналы связи и сервера, а также увеличить точность срабатывания (см. рис. 1.15 (а) и (б)).

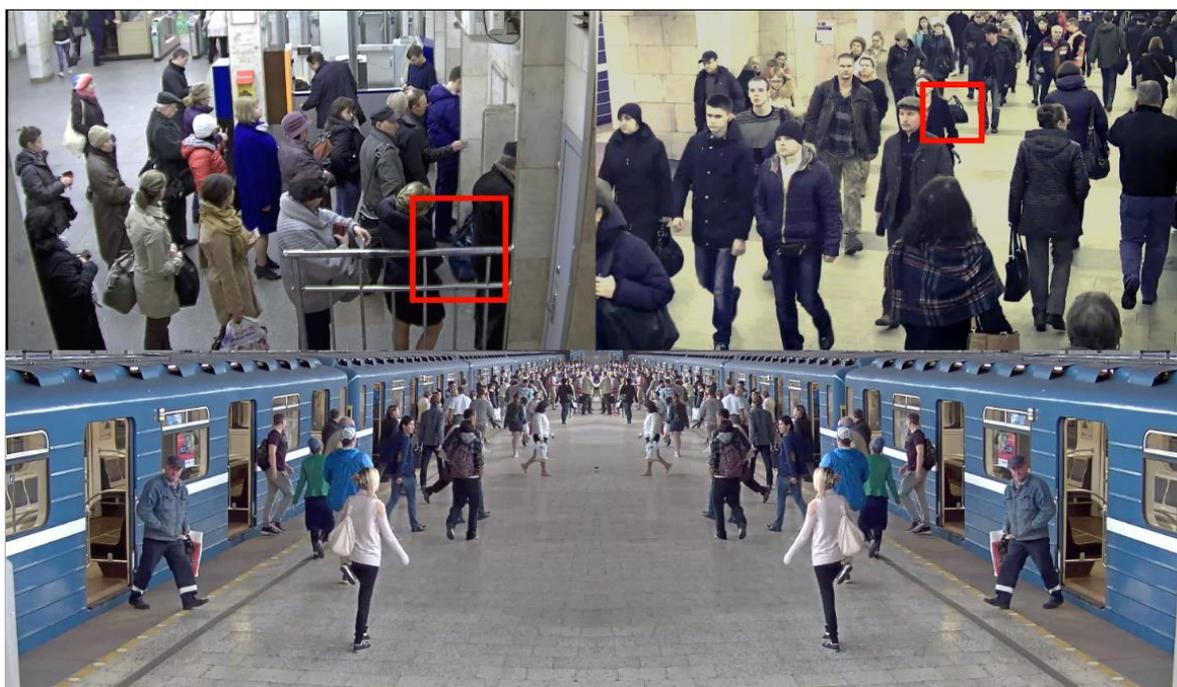


Рис. 1.15 (а). Использование детектора оставленных предметов.

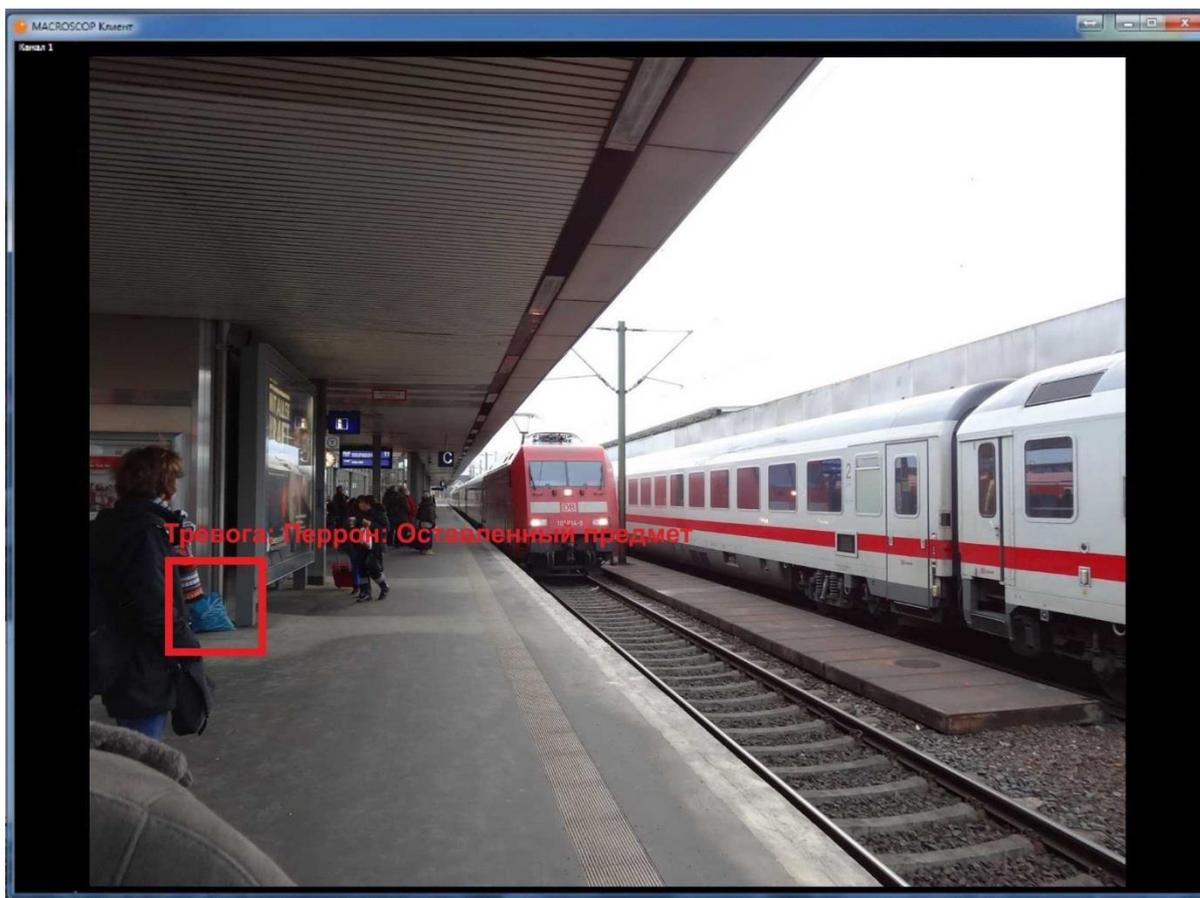


Рис. 1.15 (б). Использование детектора оставленных предметов.

Детектор драки автоматически определяет нестандартное поведение людей, связанное с хулиганством, грабежом, потасовкой. При алгоритмическом видеонаблюдении первичное обнаружение драки производит программно-аппаратный комплекс, окончательное решение принимает оператор. Так, модуль позволяет контролировать до сотни видеопотоков, не пропуская ключевых событий (см. рис. 1.16).

Принцип работы детектора драки основан на обнаружении в наблюдаемой зоне большого количества объектов или их высокой активности (быстро возникшая группа людей или активное, нестандартное поведение объекта). Распознав ситуацию по указанным признакам, видеоаналитика выдает сигнал о возникновении тревожной ситуации – драки.

Детектор драки позволяет в автоматическом режиме отслеживать все нестандартные ситуации, связанные с драками, потасовками и хулиганством, что значительно ускоряет процесс оперативного реагирования служб безопасности на данные инциденты и позволяет предотвратить их нежелательное развитие.



Рис. 1.16. Использование детектора драки.

Детектор пожара обнаруживает огонь и дым по изображению камеры, благодаря чему дальность работы детектора значительно возрастает (см. рис. 1.17). В зависимости от программной реализации такой детектор может обнаруживать следующие признаки пожара на видеопоследовательности:

- характерный цвет пламени;
- изменение контраста границ на изображении и колебания;
- турбулентное движение частиц;
- мерцание и отблески пламени.



Рис. 1.17. Работа детектора пожара.

Периметральная видеоаналитика применяется для охраны протяженных участков и периметров, обнаружения вторжения и пересечения сигнальной линии в «стерильной зоне». Особенность периметральной видеоаналитики – относительно редкие нарушения (поэтому зона называется «стерильной»), но форма и тип объекта не могут быть четко определены, например, человек может ползти или ехать на велосипеде.



Рис. 1.18. Пример работы периметральной видеоаналитики.

Охрана периметра является основным приложением профессиональной видеоаналитики. В отличие от систем видеонализа, используемых в общественных местах, видеоаналитика периметра решает более конкретную и простую задачу – первичное обнаружение человека или транспортного средства в стерильной зоне (например, на территории государственной границы, водозаборного бассейна, нефтегазопровода).

Стерильная зона, задаваемая в поле зрения камеры, предполагает отсутствие посторонних объектов на территории. При появлении таких объектов (человека, транспортного средства) система защиты периметра детектирует нештатную ситуацию и формирует сигнал оперативной тревоги, который в течение нескольких секунд (не более 10) приходит на пульт охраны (см. рис. 1.18). При этом условия обнаружения отнюдь не должны быть стерильными: допускаются помехи разного рода: животные, тени, движение растительности и дрожание камеры.

Номерная видеоаналитика применяется для распознавания регистрационных знаков автомобилей, а также для анализа их движения по данным множества камер. Система распознавания номерных знаков позволяет контролировать присутствие и перемещение транспортных средств на территории любого размера, а создание видеоархива дает возможность быстро и эффективно находить нарушителей. Интеграция системы с паркинговым биллингом сводит к минимуму влияние человеческого фактора и делает невозможным злоупотребление персоналом своими полномочиями.

Интеграция с комплексами видеофиксации нарушений ПДД обеспечивает надежный контроль над транспортными магистралями. Идентификация нарушителей по номеру позволяет автоматически подготавливать квитанции для оплаты штрафов, а также выявлять в потоке автомобили, представляющие интерес для правоохранительных органов.

Многокамерная видеоаналитика применяется для сопровождения объектов при помощи множества камер. Результатом работы многокамерной видеоаналитики является траектория движения объекта на плане всей территории наблюдения (см. рис. 1.19).

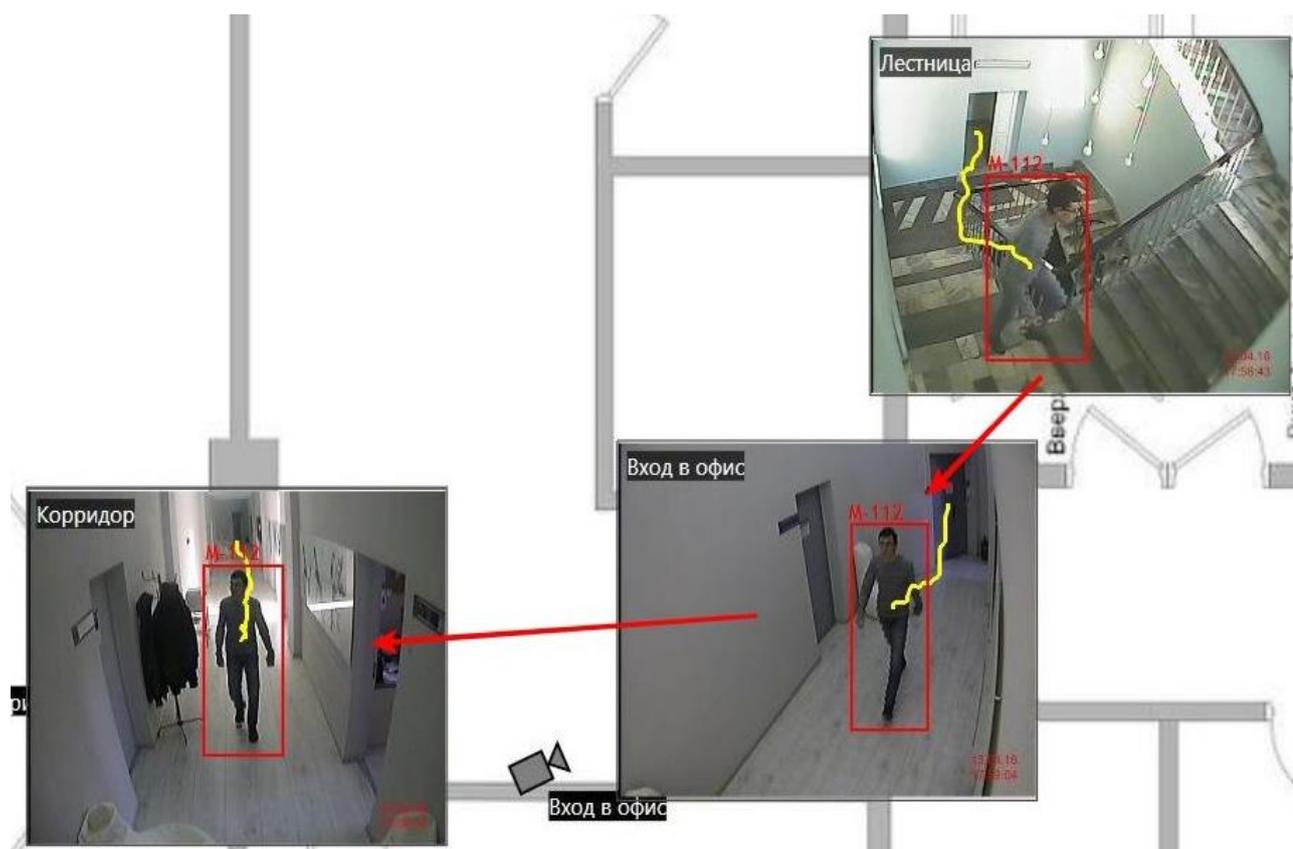


Рис. 1.19. Применение многокамерной видеоаналитики.

Необходимость в наблюдении такого типа возникает в случаях, когда наблюдаемая территория слишком велика, чтобы попасть в поле зрения одной камеры. Видеоаналитика многокамерного слежения позволяет автоматически выявлять взаимосвязи между наблюдением отдельных камер и собирать полезные данные, которые невозможно получить при помощи «однокamerной» видеоаналитики или «ручного» видеонаблюдения.

Если при однокamerном сопровождении возможна независимая обработка данных по каждому каналу, то многокамерная система должна анализировать все каналы интегрально. Многокамерное слежение учитывает трехмерную геометрию пространства и взаимное расположение телекамер, а также делает рациональные предположения о наиболее вероятной траектории движения объ-

екта, даже если он временно выходит из объединенной зоны контроля всех камер. При этом наиболее оптимальный ракурс наблюдения за человеком выбирается автоматически по мере его движения от камеры к камере.

Многокамерное слежение, а если точнее, обнаружение и сопровождение объектов, в первую очередь востребовано в таких отраслях, как охрана, безопасность, транспорт, маркетинг розничных продаж и интерактивная реклама. Для транспортной отрасли многокамерные системы позволяют отслеживать поведение пассажиров и точно измерять загрузку каждого направления на различных участках. В Лондоне и Стокгольме системы распознавания регистрационных знаков используются для контроля платы за въезд в город и при необходимости могут производить многокамерное сопровождение автомобилей в городе или вдоль трассы для спецслужб.

Интеллектуальные видеодетекторы позволяют многократно повысить продуктивность службы охраны и снизить психологическую нагрузку на операторов ситуационных центров.

Технологическая видеоаналитика применяется для мониторинга технологических процессов, обеспечения качества производства, повышения продуктивности.

Бизнес-аналитика применяется для управления организацией, оценки продуктивности персонала, оптимизации бизнес-процессов и исследований поведения клиентов. Особенность бизнес-аналитики – развитые средства обобщения данных и подготовки отчетов, иногда с возможностью исключения персональных данных.

Видеоаналитика высокой четкости применяется для видеоанализа потоков свыше одного мегапикселя (720p, 1080p и выше). Как правило, в системах видеонаблюдения высокой четкости (HD) используются принципиально новые алгоритмы, использующие многомасштабное представление видеоданных.

Тамперинг-сигнализация позволяет вести непрерывный контроль качества видеосигнала, распознавать факты несанкционированного вмешательства в работу системы видеонаблюдения либо внезапные нарушения условий наблюдения. Это могут быть, например, разворот камер, установка дезориентирующих зеркал, потеря видеосигнала, затемнение, засветка или расфокусировка изображения. Данная функция используется как для наружных камер наблюдения, так и для камер, установленных внутри помещения.

Тамперинг-сигнализация реализуется на базе сервисных детекторов:

Детектор затемнения реагирует на затемнение изображения в случаях закрытия объектива, выхода из строя устройства освещения либо системы автоматической экспозиции камеры.

Детектор засветки регистрирует направленный в объектив луч яркого света. Применяется для определения случаев умышленной или случайной засветки матрицы фоточувствительных элементов, приводящих к временной неработоспособности камеры.

Детектор расфокусировки срабатывает при потере резкости изображения по следующим причинам:

- загрязнение объектива;

- расфокусировка объектива;
- наложение на объектив линзы или фильтра;
- туман в поле зрения камеры;
- образование конденсата на оптике камеры.

Видеоаналитика своевременно регистрирует подобные явления и сообщает о них пользователю, благодаря чему видеонаблюдение может быть восстановлено без значительных временных потерь.

Технология интегрального кадра подразумевает не воспроизведение на мобильном устройстве видеопотока с камер, а отображение информативного тревожного кадра (собранного из нескольких последовательно следующих кадров тревожного события), который наглядно показывает направление движения объекта тревоги (см. рис. 1.20).



Рис. 1.20. Технология интегрального кадра.

Стоит заметить, что размер интегрального кадра составляет в среднем 50-75 КБ, а его информативность аналогична просмотру потокового видео тревожного события. Это делает данную технологию идеальным инструментом для анализа тревожных ситуаций на мобильных устройствах и позволяет пользователю принимать оперативные и оптимальные решения.

Биометрическая видеоаналитика применяется для идентификации и сопровождения лиц по биометрическим признакам лица. Классическая биометрия использует «черный» и «белый» списки для сравнения изображений людей. Биометрическая видеоаналитика может работать по более сложным сценариям, например, осуществлять профайлинг людей или сопоставляет наблюдения множества камер в территориально-распределенной сети наблюдения.

Детектор лиц обеспечивает обнаружение и сопровождение всех лиц, попадающих в поле зрения камеры. Все лица хранятся в архиве, благодаря чему можно в любой момент найти людей, посетивших объект, например, за определенный промежуток времени, или через конкретный вход. Алгоритм оптимизи-

рован для камер сверхвысокого разрешения, используемых в существующих системах распознавания лиц.

Автоматизированные программно-аппаратные комплексы биометрической идентификации по лицу человека (далее – АПКБИ) предназначены для выявления в потоке пассажиров и других посетителей вокзальных комплексов лиц, которые находятся в розыске или представляют оперативный интерес для органов внутренних дел. Выявление происходит путем сравнения изображения лица, входящего в вокзал с фотографией, имеющейся в базе данных комплекса (см. рис. 1.21). После выявления осуществляется информирование сотрудников полиции об этом факте и дальнейшее сопровождение или задержание разыскиваемого лица.

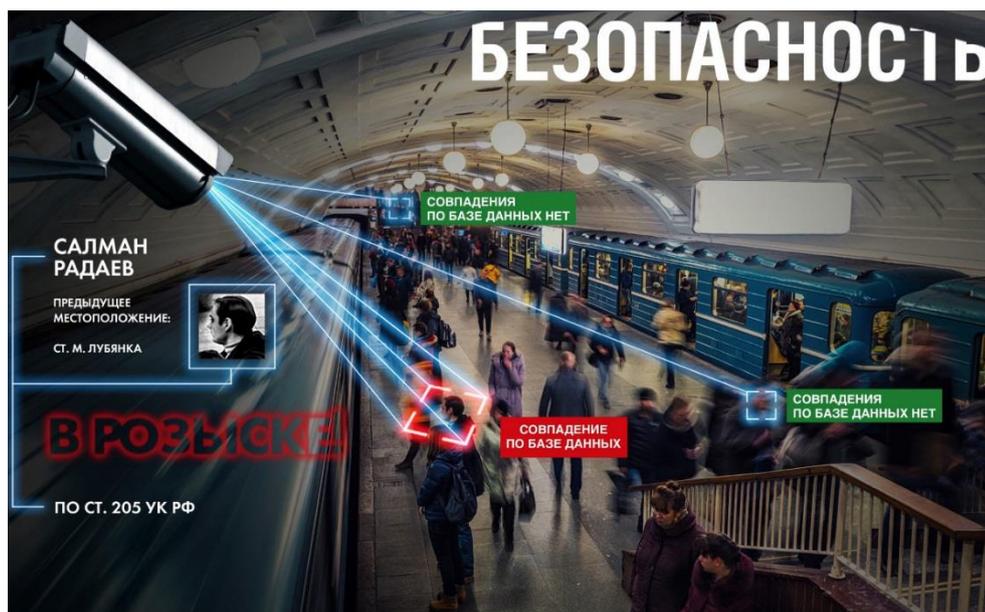


Рис. 1.21. Работа комплекса автоматизированной биометрической идентификации по лицу человека.

Для выявления людей с помощью АПКБИ используются установочные данные, в качестве которых выступают ФИО и паспорт человека. Эти данные берутся из массивов проданных железнодорожных, авиационных, морских и речных билетов. Кроме того, в базе данных используются фотографии лиц, находящихся в розыске, или представляющих оперативный интерес для органов внутренних дел.

АПКБИ используют новейшие передовые информационные технологии, ультрасовременные разработки в области микропроцессорной техники, а также наукоемкие и быстрые алгоритмы биометрической идентификации. Это позволяет им в режиме реального времени выявлять в пассажиропотоке, входящем или выходящем, на объектах транспорта, лиц, находящихся в розыске или представляющих оперативный интерес.

Рассмотрев общие особенности организации обеспечения безопасности с использованием видеонаблюдения и видеоаналитики, мы можем перейти к выявлению технических средств и программного обеспечения, которые должны использоваться в системах видеонаблюдения и видеоаналитики аэропортов для решения поставленных задач.

Контрольные вопросы:

1. Указать нормативную правовую базу, регулирующую техническое обеспечение и использование технических средств на объектах транспортной инфраструктуры, относящихся к воздушному транспорту.
2. Перечислить критерии категорирования ОТИ аэропортовых комплексов.
3. Перечислить и охарактеризовать классификацию аэропортов.
4. Перечислить компоненты системы технического обеспечения транспортной безопасности.
5. Назвать принципы построения системы видеонаблюдения.
6. Перечислить характеристики видеокамер.
7. Охарактеризовать виды компрессии видеосигнала.
8. Описать возможности систем видеонаблюдения и контроля удаленным доступом.
9. Перечислить и охарактеризовать модули видеоаналитики.
10. Перечислить виды детекторов, используемых в ситуационной видеоаналитике.

2. ТЕХНИЧЕСКИЕ СРЕДСТВА И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ИСПОЛЬЗУЕМЫЕ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ И ВИДЕОАНАЛИТИКИ АЭРОПОРТОВ

2.1. Элементы системы видеонаблюдения аэропорта: технические характеристики и особенности применения

В первой главе рассмотрены требования к системам видеонаблюдения в зависимости от категории аэропорта и общие принципы построения систем видеонаблюдения.

Аэропорт – это один из самых сложных объектов гражданской инфраструктуры с точки зрения обеспечения безопасности. Безопасность аэропорта необходимо начинать контролировать не с прохождения предполетного досмотра и даже не с входа в здание аэровокзала, а с прилегающих территорий. Здесь располагаются остановки общественного транспорта, парковки личного транспорта и происходит постоянное перемещение людей и транспорта.

Современная система видеонаблюдения аэропорта – это комплекс программно-аппаратных средств, центрального оборудования и камер видеонаблюдения с широкими функциональными возможностями. Следует помнить, что любая надежная система видеонаблюдения должна иметь и современную инфраструктуру передачи сигнала. Рассмотрим подробнее задачи и требования, которые предъявляются к системам видеонаблюдения в аэропортах сегодня.

Характеристики камер видеонаблюдения

Безусловно, первым параметром, по которому производится подбор камеры видеонаблюдения, является фокусное расстояние объектива, определяющее ее угол обзора, степень детализации изображения¹².

Также в зависимости от условий эксплуатации камеры, задач, стоящих перед системой видеонаблюдения, следует знать про ряд других, описанных ниже, технических характеристик и параметров.

Чувствительность.

Способность видеокамеры создавать изображения с необходимой подробностью в условиях недостатка освещения имеет важнейшее значение во многих системах наружного видеонаблюдения.

¹² Жукова П.Н., Насонова В.А., Прокопенко А.Н. Возможности использования информационных технологий при борьбе с организованной преступностью на объектах транспортной инфраструктуры / Математические методы и информационно-технические средства: материалы XII Всероссийской научно-практической конференции (Краснодар, 17 июня 2016 г.). – Краснодар: Краснодарский университет МВД России, 2016. С. 105-109.

К сожалению, единый стандарт измерения чувствительности в CCTV индустрии отсутствует. Производители видеокамер приводят значения чувствительности, измеренные по собственным методикам. Значения чувствительности, приведённые в спецификациях многих производителей, соответствуют изображению, на котором на фоне сильного шума с трудом можно различить лишь силуэты крупных высококонтрастных объектов.

Мало кто из производителей приводит значения чувствительности, измеренные согласно открытым стандартам.

В итоге, у видеокамер с фактически одинаковой чувствительностью, но выпущенных разными производителями значения в спецификации могут отличаться в десятки раз.

Частота кадра.

Даже если IP-камера способна передавать качественную картинку в сложных условиях наблюдения, тем не менее полезная информация может быть утеряна, потому что IP-камера сформировала изображение с низкой частотой кадров, например, 6 или 12 к/с и не успела зафиксировать нужные детали. Это актуально и при наблюдении автомобильного трафика, когда из-за высокой скорости транспортных средств и особенностей установки IP-камер с различными ракурсами автомобили пересекают область наблюдения за очень короткий интервал времени. Поэтому в определенных случаях могут потребоваться устройства, которые формируют изображение с высокой частотой кадров. Сейчас на рынке систем видеонаблюдения все чаще появляются мегапиксельные камеры, способные формировать изображение со скоростью до 60 к/с. При использовании таких моделей система не пропустит важные детали, даже когда в поле зрения камер будут появляться быстро движущиеся объекты.

Разрешение.

Разрешение определяет степень детализации изображения, формируемого камерой видеонаблюдения, причем этот параметр определяется несколькими факторами:

- характеристиками матрицы камеры;
- объективом (его качеством, фокусным расстоянием);
- дистанцией до наблюдаемого объекта.

Наличие ИК подсветки.

Чтобы система видеонаблюдения всегда оставалась эффективной, зачастую используется внешнее освещение белого света, причем для таких случаев даже имеются специальные нормы по уровню освещенности. Однако на практике далеко не всегда выполняются эти условия. К тому же мощные источники видимого света могут оказывать и негативное влияние, например, слепить встречным светом водителей. Поэтому в системах видеонаблюдения очень распространена ИК-подсветка, которая невидима человеческому глазу, но хорошо воспринимается матрицами современных IP-камер. Также ИК-излучение хорошо отражается от таких объектов, как, например, автомобильные номера, что делает ее еще более эффективной. Тем не менее и в данном случае имеются свои особенности - для эффективной круглосуточной работы камеры видеонаблюдения в темное время

суток мощность подсветки должна быть распределена равномерно по всему полю ее обзора. Только тогда изображение будет хорошо различимо целиком.

Автоматическая регулировка диафрагмы.

Диафрагма объектива – это устройство, устанавливаемое обычно внутри объектива и управляющее размером создаваемого отверстия, через которое свет попадает на светочувствительную матрицу и, соответственно, регулирующее количество света, проходящее к светочувствительной матрице.

Диафрагма сильно влияет на конечное изображение, получаемое с видеокамеры. Малая величина значения диафрагмы означает, что объектив пропускает больше света, что улучшает изображение, даваемое камерой видеонаблюдения в условиях слабой освещенности (например, ночью). Большая величина значения диафрагмы уменьшает световой поток, попадающей на светочувствительную матрицу, предотвращая «ослепление» камеры видеонаблюдения высокой освещенности (например, если камера направлена на окно комнаты) и поддерживает постоянный уровень яркости видеоизображения.

Управление количеством проникающего через объектив света осуществляется путём регулировки диафрагмы объектива.

Если камера видеонаблюдения устанавливается в помещении с постоянным уровнем освещения, то можно использовать ручную регулировку диафрагмы.

В этом случае для регулировки диафрагмы следует просто поворачивать кольцо диафрагмы до тех пор, пока изображение от камеры не станет хорошо передавать различные оттенки.

Если камера будет устанавливаться на улице или в условиях частого изменения уровня освещенности, необходимо использовать объективы с автоматической регулировкой диафрагмы.

Электронный затвор.

Определяет промежуток времени, в течение которого матрица накапливает сигнал. Принцип действия аналогичен затвору фотоаппарата. Регулировка диафрагмы предназначена для обеспечения работы камеры при разном уровне освещения, однако АРД эффективнее.

Электронный затвор – устройство, предназначенное для ее адаптации к изменениям уровня освещенности.

Компенсация засветки (заднего света).

Позволяет вести видеонаблюдение за объектом, сзади которого находится яркий источник света.

Необходимость использования компенсации засветки продиктована невозможностью одинаково четкой передачи деталей ярких и темных элементов изображения. Так как камера изменяет значения выдержки и управляет диафрагмой, основываясь на средней яркости сцены, нередко возникают ситуации, когда яркие объекты (лампы, мониторы и т.д.), попав в поле зрения камеры, приводят к неразличимости деталей в темных участках. Для того, чтобы детали в темных тонах были лучше различимы, необходимо убрать из расчета средней яркости данные источники света. Функция компенсации яркой засветки делает это, маскируя яркие источники света маской.

Автоматический баланс белого.

Баланс белого – это функция видеокамеры, предназначенная для компенсации искажения различных цветов, которые возникают при разных источниках освещения. Видеосъемка может производиться при солнечном свете, в помещении, освещенном лампой накаливания, люминисцентной или галогеновой лампой, вечером при свете костра и пр. Каждый источник света обладает своим спектром излучения. Во всех современных видеокамерах есть функция автоматического баланса белого цвета, направленная на воспроизведение относительно естественных цветов. Однако автоматика не всегда в состоянии правильно отреагировать на разнообразные источники освещения. Если белый предмет на видео имеет желтый, синеватый или другие оттенки, это вызвано освещением и требует настройки, т.е. установки баланса белого. Типичный пример, когда съемка при домашнем освещении дает характерное отображение объектов в желтоватых тонах.

Виды камер видеонаблюдения, используемые для обеспечения безопасности в аэропорте

Построение системы видеонаблюдения осуществляется в соответствии с общей концепцией охраны объекта транспортной инфраструктуры. Указанная концепция формируется на основе категории аэропорта и определяет выбор и расположение используемого оборудования. Однако при любой концепции оборудованию системой видеонаблюдения подлежат:

- периметр аэропорта;
- центральный вход в здание аэровокзала;
- коридоры на этажах аэровокзала;
- помещения в зданиях, обязательные для видеонаблюдения.

Рассмотрим общие особенности формирования систем видеонаблюдения в указанных зонах.

Аэропортовый комплекс включает в себя множество распределенных разнородных подобъектов, следовательно, использование большого количества и разновидности видеокамер полностью обусловлено, поскольку обслуживание компонентов системы должно быть минимальным.

Выбор расположения и качества установленной системы видеонаблюдения определяется расположением объекта, его протяженностью, пропускной способностью пассажиропотка, загруженностью в различное время суток.

Таким образом, система видеонаблюдения подразделяется, в соответствии с обеспечением безопасности аэропортового комплекса, на несколько рубежей:

- участок дороги к аэропорту;
- территория аэровокзального комплекса;
- здание аэровокзала;
- видеонаблюдение за взлетно-посадочной полосой и рулежными дорожками;
- система охраны периметра.

Обеспечение безопасности аэропорта начинается *на подъезде к объекту транспортной инфраструктуры*.

На данном этапе построения системы видеонаблюдения применяются те же принципы, что и для дорожного видеонаблюдения. Соответственно камеры должны:

- быть поворотными (классические поворотные камеры с щеткой-очистителем смотрового окна камеры). *Не применимы купольные поворотные камеры*, так как купола неизбежно и достаточно быстро загрязнятся;
- обладать высоким разрешением не менее 2-х мегапикселей;
- иметь высокую чувствительность для съемки в сложных условиях освещенности;
- обладать оптическим зумом не менее 30-ти крат;
- быть оснащенными электронным или механическим стабилизатором изображения.

На *территории аэровокзального комплекса*, включая парковочную зону, должна быть создана автоматизированная система контроля доступа и парковочная система, которая будет интегрирована с системой видеонаблюдения и видеокамерами, способными распознать номерные знаки автомобилей. Кроме того, для аэропортов первой и второй категории (и по возможности третьей) эта автоматизированная система должна быть со встроенной видеоаналитикой, позволяющей отследить остановку/парковку в неправильном месте, пересечение сплошных линий, движение по полосе встречного движения, подсчет автомобилей, так называемое праздношатание на парковке и, наконец, оставленные предметы¹³.

Наибольшее же сосредоточение камер находится в самом *здании аэровокзала*. При входе в здание аэропорта пассажиры подвергаются первому досмотру. Для аэропортов первых двух категорий у каждого пункта досмотра должны быть установлены камеры, которые позволяют распознавать лицо человека и, при совпадении с данными из баз данных, выявлять потенциально опасных людей. Для аэропортов третьей, четвертой и пятой категорий камеры должны просто снимать всех лиц, входящих в здание.

В здании аэровокзала важно перекрыть все зоны стационарными камерами и продублировать поворотными. Большинство аэропортов имеют очень высокие потолки и большие открытые площади залов регистрации и залов ожидания, поэтому именно в аэропортах целесообразно использовать многосенсорные многомегапиксельные (12 Мп и выше) панорамные камеры с углом обзора по горизонтали 180, 270 или 360 градусов, и в этом случае нельзя забывать о задних засветках от окон здания аэровокзала. Именно в здании аэровокзала, в первую очередь, востребованы такие функции видеоаналитики, как оставленные предметы, подсчет людей, детектирование очередей, наиболее популярных мест (построение тепловых карт), скопление людей. Для поворотных камер очень полезной видеоаналитической функцией оказывается адаптивное авто-

¹³ Жукова П.Н., Насонова В.А., Прокопенко А.Н. Обеспечение безопасности на объектах транспортной инфраструктуры посредством использования систем видеонаблюдения и видеоаналитики // Проблемы правоохранительной деятельности. 2015. № 4. С. 91-96.

слежение, т.е. выбор цели по заданным параметрам и дальнейшее ее ведение, до появления более подходящей цели.

Особо следует отметить кабинки пограничного контроля, здесь необходимым условием является съемка как сотрудника пограничной службы, так и проходящего пассажира. И обязательным условием является запись звука с камер. При этом запись звука с других камер может быть не обязательной, но желательной. Чаще начинает использоваться звуковая аналитика, которая позволяет реагировать и подавать сигнал на определенные звуки, например, резкие хлопки или даже конкретные слова.

Также камеры по внешним признакам, с помощью специальных видеоаналитических алгоритмов, позволяют выявлять людей с нестабильным психоэмоциональным состоянием. Обычно внутри аэровокзала используются камеры не более 2-х мегапикселей, но с высокой чувствительностью, так как в большинстве случаев камера ведет съемку людей в условиях задней засветки от яркого дневного света, попадающего через стеклянные двери.

Кроме того, на входе в аэровокзал все чаще устанавливают тепловизоры с термографической видеоаналитикой, которые позволяют выявить больных людей с повышенной или, наоборот, пониженной температурой тела относительно нормы. Наконец, камеры на входе могут считать людей, а также помогать следить за образующимися очередями на пропускных пунктах и подавать сигнал о необходимости открытия дополнительных пунктов пропуска.

Система видеонаблюдения за взлетно-посадочной полосой и рулежными дорожками

Обычно описание систем видеонаблюдения аэропорта ограничивается рассмотрением соответствующего оборудования и видеокамер в здании аэровокзала. Но не менее сложной и интересной является задача видеонаблюдения за взлетно-посадочной полосой и рулежными дорожками. Тем более что видеосъемка осложняется в ночное время суток, в связи с определенными требованиями ИКАО по освещению взлетно-посадочных полос и рулежных дорожек. Согласно этим требованиям источники видимого и инфракрасного света должны располагаться не выше определенной высоты и под определенным углом, чтобы не быть помехой для посадки воздушных судов, результатом чего является большое количество абсолютно не освещенных мест, за которыми также необходимо вести съемку и в темное время суток, и во время тумана.

Поэтому для наблюдения за этими зонами применяют поворотные тепловизионные камеры для съемок при плохой видимости и поворотные некупольные видеокамеры для съемки при достаточной видимости. Также тепловизоры кроме охранных могут выполнять и другие функции, например, реагировать на перегревы, открытое пламя или следить за наполненностью цистерн с горючим.

Система охраны периметра

Необходимый рубеж охраны аэропорта – система охраны периметра. Здесь вдоль всего забора применяют стационарные тепловизоры с видеоаналитикой, причем сложность конфигурации забора практически не важна. Всю сцену съемки тепловизора делят на зоны детекции движения, при сработке одной из них оператору подается сигнал, и в это место позиционируется поворотный тепловизор с узкоугольным объективом для наблюдения за удалёнными объектами или обычная поворотная видеокамера, и это изображение также выводится оператору.

Особо важным является выбор самой системы видеонаблюдения. Для объекта такого масштаба, как аэропорт, и сама СВ должна быть свободно масштабируемой. То есть при развитии аэропортового комплекса, например, при строительстве новых терминалов, должна пропорционально расти система видеонаблюдения.

Причем, как и объекты аэропорта распределены по значительной территории, так и компоненты единой системы видеонаблюдения должны быть распределенными, а в случае необходимости должны иметь возможность работать автономно от общей системы. За каждую часть аэропорта отвечает своя служба обеспечения безопасности, и чем он больше, тем этих служб больше. Поэтому важно, чтобы была возможность гибко настроить права доступа к видеосистеме, и при этом операторских мест должно быть сколько угодно много (на объектах подобного плана, с которыми приходилось сталкиваться, количество мест операторов достигало 50-ти). Кроме того, если аэропорт является международным, зачастую, зона пограничного контроля охраняется автономными системами безопасности, т.к. эта зона ответственности лежит на сотрудниках службы пограничного контроля ФСБ. В идеале, система видеонаблюдения должна быть унифицирована для всех зон аэропорта, в том числе и зон пограничного контроля.

Кроме свободной масштабируемости, СВ должна обладать широкими возможностями по интеграции со сторонними системами безопасности и автоматизации, такими как система контроля доступа аэропорта, система автомобильной парковки, периметральная система охраны, система сбора маркетинговых данных, системы автоматизации освещения и климата зданий и так далее.

Так как транспортные объекты являются критически важными, все системы должны иметь резервирование, и это тот случай, когда можно сказать, что резервирования «много не бывает». В системах для аэропортов особое внимание должно уделяться резервированию архивов и серверов, на которых этот архив хранится. Поэтому в самих серверах применяют резервирование дискового пространства RAID6, резервирование всех охлаждающих кулеров, блоков питания. Все сервера системы видеоменеджмента резервируют по схеме N+1, в наиболее продвинутых системах сервера объединяют в IT-кластеры, которые также резервируют. Ну и наконец, в целом ЦОДы и распределенные элементы системы резервируют с помощью источников бесперебойного питания.

Создание такой сложной системы, как система видеонаблюдения аэропорта, требует большой подготовительной работы. В проекте должны быть предусмотрены и обоснованы:

- выбор оборудования и общего построения системы;
- точки расположения камер, с указанием направления и сектора обзора;
- способ крепления камер;
- тип и способы подключения прокладываемых линий связи;
- активное оборудование передачи данных (с расчетом передаваемых потоков и нагрузки на сеть);
- оборудование записи видео (с расчетом требуемого объема системы хранения в зависимости от желаемой глубины архива в днях);
- размещение мест операторов и связь с ними;
- состав каждого рабочего места оператора (количество мониторов, их размещение; аппаратное и программное обеспечение);
- расположение стойки или шкафа с центральным оборудованием;
- размещение оборудования в нем.

Аэропортовый комплекс включает в себя множество разнородных подобъектов, таким количеством разновидностей видеокамер не сможет похвастаться ни один другой тип объектов. В связи с большой распределенностью аэропортовых объектов важно, чтобы обслуживание компонентов системы было минимальным. Обеспечение безопасности аэропорта начинается еще на трассах, ведущих к нему, где применимы те же принципы выбора камер, что и для дорожного видеонаблюдения¹⁴.

Камеры должны быть поворотными, обладать высоким разрешением не менее **2-х мегапикселей**, обязательно высокой чувствительностью для съемки в сложных условиях освещенности, **оптическим зумом не менее 30-ти крат** и, соответственно, электронным или механическим стабилизатором изображения, иначе от вибраций от проезжающих автомобилей при максимальном зуме оператор увидит дрожащую и абсолютно не информативную картинку. Приезжающий автомобиль встречают автоматизированная система контроля доступа на территорию аэровокзального комплекса и парковочная система, которая обязательно интегрирована с системой видеонаблюдения и видеокамерами, способными распознать номерные знаки автомобилей. Кроме того, все чаще применяют камеры со встроенной видеоаналитикой, позволяющей отследить остановку и парковку в неправильном месте, пересечение сплошных линий, движение по полосе встречного движения, подсчет автомобилей и оставленные предметы.

¹⁴ Постановление Правительства Российской Федерации от 23 января 2016 Г. № 29 «Об утверждении требований по обеспечению транспортной безопасности объектов транспортной инфраструктуры по видам транспорта на этапе их проектирования и строительства и требований по обеспечению транспортной безопасности объектов (зданий, строений, сооружений), не являющихся объектами транспортной инфраструктуры и расположенных на земельных участках, прилегающих к объектам транспортной инфраструктуры и отнесенных в соответствии с земельным законодательством Российской Федерации к охраняемым зонам земель транспорта, и о внесении изменений в Положение о составе разделов проектной документации и требованиях к их содержанию» // Собрание законодательства Российской Федерации. 2016. № 5. Ст. 698.

Все это движение необходимо отслеживать в хорошем разрешении с одновременной непрерывной записью в максимальном качестве. Причем оператор видеонаблюдения должен иметь возможность видеть, как всю территорию, так и отдельные зоны в увеличенном масштабе.

От обзорных камер требуется, чтобы они хорошо работали в сложных условиях освещенности и выдавали качественное изображение. В последнее время шла активная борьба за качество видеоизображения, которое складывается из двух определяющих факторов - разрешения и чувствительности камеры. На сегодняшний день стандартом стали камеры видеонаблюдения с высокоточным разрешением (HD), которые дают более качественное изображение, чем камеры предыдущего поколения.

Это можно реализовать, например, при помощи профессиональной IP-камеры (см. рис. 2.1) Axis Q1755-E с разрешением 1080i или 720p, 10-кратным оптическим и 12-кратным цифровым зумом, смонтированной в корпусе с классом защиты IP66, обеспечивающую работу камеры при температуре до -40С.



Рис. 2.1. Профессиональная поворотная IP-камера.

Для охраны периметра от несанкционированного пересечения также можно использовать фиксированные IP-камеры, расположенные на опорах вдоль ограждения. Здесь можно с успехом применить камеры Axis P1354-E, P1355-E или Q1755-E.

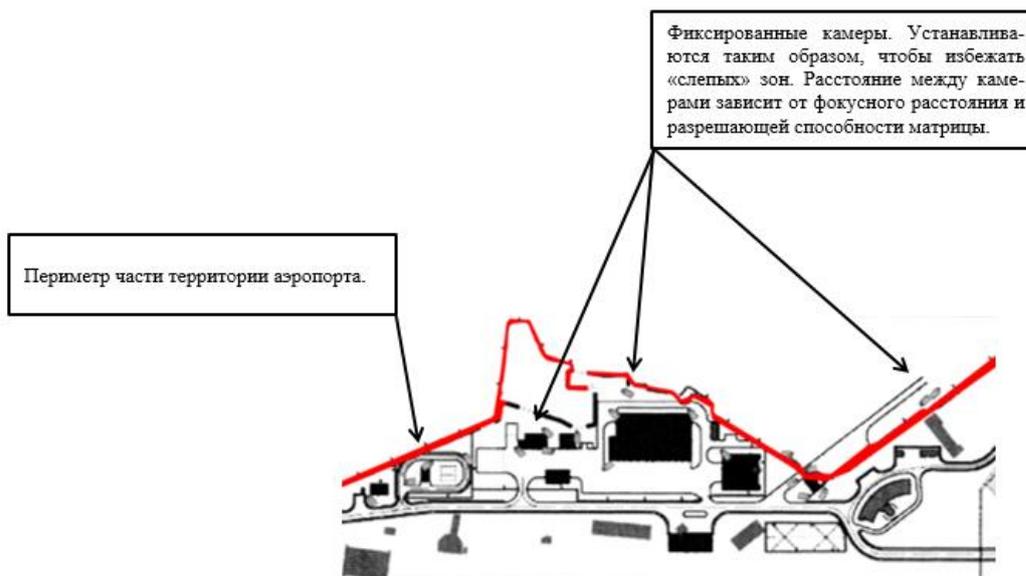


Рисунок 2.2. Схема расположения видеокамер по периметру аэропорта.

Наибольшее сосредоточение камер находится в самом здании аэровокзала (см. рис. 2.2). При входе в здание аэропорта пассажиры подвергаются первому досмотру. У каждого пункта досмотра установлены камеры, которые позволяют распознавать лицо человека и, при совпадении с данными из баз данных, выявлять потенциально опасных людей.

Территория аэропорта должна контролироваться таким образом, чтобы слепые зоны отсутствовали, то есть камеры должны быть фиксированными. Только если вся территория просматривается фиксированными камерами, допускается установка поворотных камер (см. рис. 2.3).

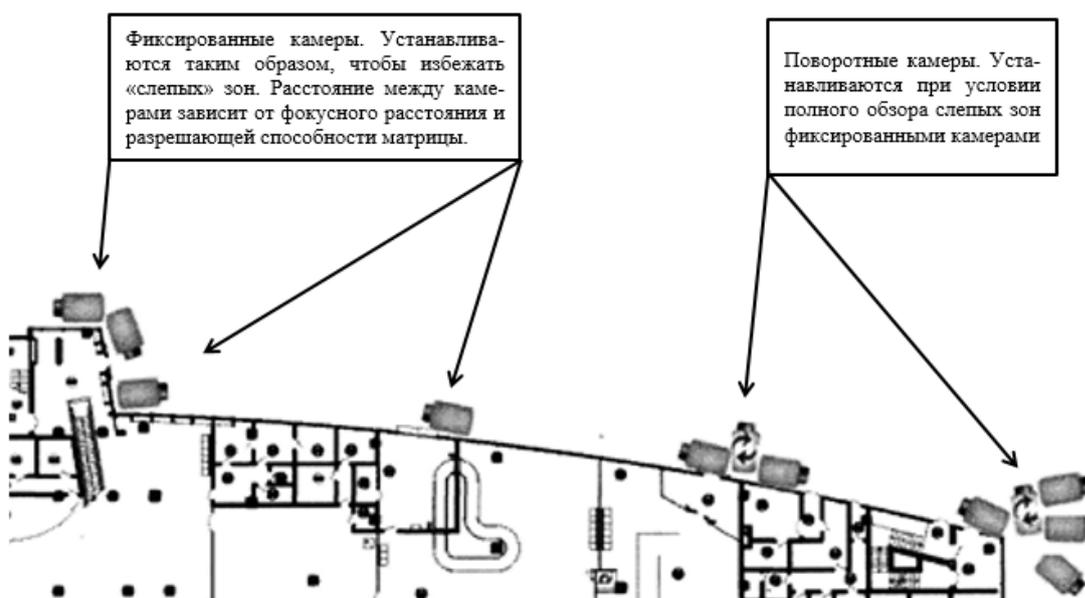


Рисунок 2.3. Схема расположения охранных видеокамер по периметру аэровокзала.

Внутри аэровокзала не должно быть ни единого места, за которым бы не велась видеосъемка. Часто можно услышать мнение, что достаточно купольных поворотных камер с хорошим оптическим зумом, но это абсолютно не верно, так как наличие мертвой зоны у поворотной камеры может повлечь несанкционированный проход посторонних лиц в специальные зоны с помощью работника аэропорта. Поэтому в аэропорте важно перекрыть все зоны стационарными камерами и продублировать поворотными (см. рис. 2.4).

Следует особо отметить кабинки пограничного контроля, здесь необходимым условием является съемка как сотрудника пограничной службы, так и проходящего пассажира, и обязательным условием является запись звука с камер. При этом, запись звука с других камер может быть не обязательной, но лишней также не будет, тем более что все большую популярность набирает звуковая аналитика, которая позволяет реагировать и подавать сигнал на определенные звуки, например, резкие хлопки или даже конкретные слова.



Рисунок 2.4. Схема расположения видеокamer в здании аэровокзала.

В коридорах и технических помещениях эффективны будут фиксированные камеры. Распознавание лиц в этих помещениях использоваться не будут, следовательно, нет необходимости использовать камеры высокого разрешения. В данном случае с поставленной задачей справится камера RVi-IPC41S V.2 (см. рис. 2.5).



Рисунок 2.5. Охранная видеокамера RVi-IPC41S V.2.

Интеллектуальные камеры видеонаблюдения, которые снабжены заранее встроенным датчиком-видеоаналитиком, способны обнаружить подозрительное поведение и предупредить службу безопасности аэропорта заблаговременно. Эти камеры запрограммированы на обнаружение конкретных видов деятельности (см. рис. 2.6).

Технические помещения и коридоры.



Рисунок 2.6. Схема расположения видеокамер в технических помещениях и коридорах.

Любые перемещения воздушных судов по территории аэропорта, техническое обслуживание и прочие мероприятия должны непрерывно записываться системой. Причем запись должна быть в максимально высоком качестве, что может быть полезным для детального изучения в случае каких-либо нарушений или чрезвычайных ситуаций (см. рис. 2.7).

Прилегающая территория и взлётно-посадочная полоса

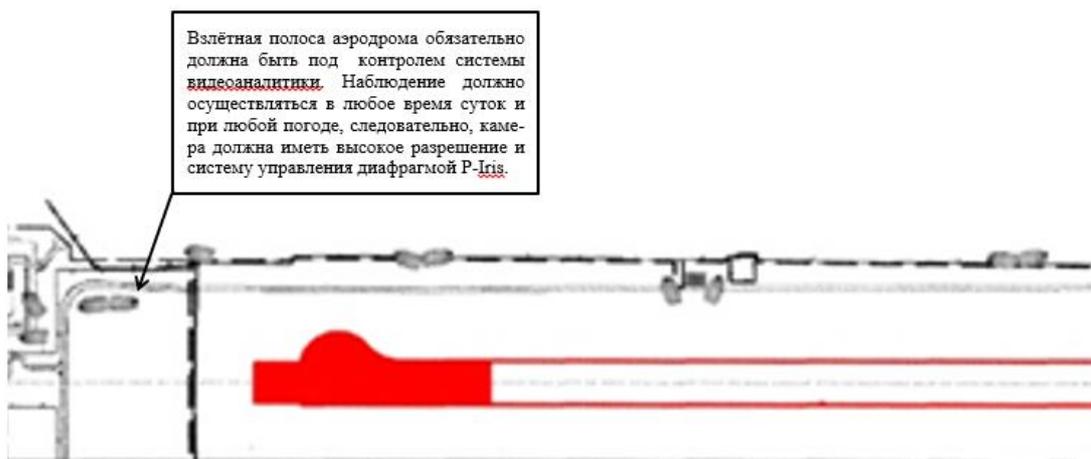


Рисунок 2.7. Схема расположения камер на территории аэропорта.

Для данных целей прекрасно подойдет камера Axis P3367-VE с разрешением 1080р, обеспечивающая два независимых потока H.264 и Motion JPEG и поддерживающая технологию управления диафрагмой P-Iris. Система P-Iris обеспечивает четкое контрастное изображение с большой глубиной резкости в любых условиях освещения. А также камеры Axis P3304-V, в качестве экономичного решения или Axis P3367-V – высококачественная модель с Full HD разрешением, современными функциями обработки изображения и множеством интеллектуальных возможностей (см. рис. 2.8).



Рис. 2.8. Профессиональная купольная поворотная IP-камера.

Одной из самых перспективных и удачных разработок можно считать мультиматричное видеонаблюдение. Данная технология может быть использована, в частности, для наблюдения за лётными полями (аэродромами). Система Rapomera прошла успешное внедрение для организации видеонаблюдения за привокзальной площадью и зонами парковок.

Одной из важнейших задач обеспечения безопасности воздушных судов является оснащение диспетчерских пунктов, отвечающих за взлет и посадку воздушных судов, системами видеонаблюдения. В данном случае система видеонаблюдения может значительно облегчить работу этим службам, уменьшить время реакции на событие, получить данные для оптимизации работы. Благодаря нескольким «камерам» внутри такой системы задний план не теряет четкости изображения (разрешения). При этом линии связи достаточно проложить в одну-две точки, что экономически оправдывает решение на базе Panomera в сравнении с традиционной системой видеонаблюдения, для создания которой потребуется проложить большое количество кабелей и перерыть для это значительные территории на лётном поле (см. рис. 2.9).



Рисунок 2.9. Мультиматричное видеонаблюдение Panomera.

Камеры видеонаблюдения обеспечивают мониторинг нескольких участков одновременно. Развертывание камер видеонаблюдения необходимо на всех ключевых участках аэропорта, чтобы операторы могли контролировать различные виды деятельности и принять соответствующие меры в случае возникновения такой необходимости. Интеллектуальные камеры видеонаблюдения, которые снабжены заранее встроенным датчиком-видеоаналитиком, способны обнаружить подозрительное поведение и предупредить службу безопасности аэропорта заблаговременно. Эти камеры запрограммированы на обнаружение конкретных видов деятельности.

2.2. Элементы системы видеоаналитики аэропорта: технические характеристики, программное обеспечение и особенности применения

Как правило, в состав комплекса входят следующие составляющие:

- IP-видеокамеры высокого разрешения (не менее 2-5 мрх), фиксирующие лица всех входящих в здание вокзала граждан. Устанавливаются на пунктах контроля;
- серверы биометрической идентификации (1 сервер на 5-6 видеокамер), использующие наиболее эффективные на настоящее время алгоритмы биометрической идентификации. На серверах хранится база данных фотографий, с которыми осуществляется сравнение. Размещаются серверы в отдельном шкафу в помещении серверной дежурной части полиции;

– автоматизированные рабочие места – для контроля работы системы и информирования дежурного сотрудника ОВД о выявлении разыскиваемого лица. Как правило, АРМ устанавливаются в дежурной части полиции или, в отдельных случаях, в специально оборудованных пунктах полиции в разных частях вокзала (в большом объекте транспортной инфраструктуры, например, международном аэропорте);

– носимые устройства оповещения о выявлении разыскиваемого – для извещения нарядов полиции о выявлении разыскиваемого в пассажиропотоке и демонстрации изображения пассажира, требующего проверки. Устройства находятся у полицейских, патрулирующих здание вокзала;

– коммутационное оборудование;

– источники бесперебойного питания;

– дополнительное осветительное оборудование для обеспечения в зоне наблюдения освещенности, достаточной для успешной идентификации.

Для нормальной работы комплекса необходимо выполнение ряда условий технического характера.

Во-первых, скорость реакции комплекса на выявление разыскиваемого лица с момента прохода перед камерой идентификации не должна превышать 3-5 секунд для одиночного выявления. В случае группового выявления скорость реакции комплекса не должна превышать 7-10 секунд. Это требование обусловлено тем, что за указанный отрезок времени выявленное лицо не должно успеть уйти далеко от видеокамеры. В противном случае оно может скрыться внутри объекта транспортной инфраструктуры, например, в туалете, магазине, пункте общественного питания, камере хранения и т.д. Особенно критичной скоростью выявления лиц является в метро и при выявлении террористов.

Во-вторых, скорость обработки данных с одной камеры должна превышать 5 кадров в секунду. Это позволит охватить весь транспортный поток входящих лиц.

В-третьих, объем базы разыскиваемых лиц должен составлять от 10 тысяч до 250 тысяч человек. Если база данных превышает 250 тысяч человек, то возникает необходимость существенного увеличения привлекаемых серверных мощностей. Это ведет к дополнительным финансовым затратам. При этом использование поисковой базы объемом менее 5 тысяч человек является неэффективным, поскольку обнаружение будет происходить очень редко. В этой связи создающие запросы на поиск сотрудники должны ответственно подходить к размещению в базе данных лиц. Кроме того, необходимо своевременное удаление лиц, поиск которых прекращен. Общее количество лиц, которых можно занести в базы данных, у разных комплексов составляет от 1 до 5 миллионов записей. Однако оперативно использоваться должна только часть записей¹⁵.

¹⁵ Жерновой М.В., Сухаренко А.Н. Проблемы борьбы с организованной преступностью в СНГ // Российская юстиция. 2012. № 6. С. 37-40.

В-четвертых, комплексы предъявляют существенные требования к качеству фотографий разыскиваемых лиц. Расстояние между зрачками человека должно быть не менее 90 пикселей (рекомендуется 120-150). Лицо должно находиться в положении фас с углом поворота или наклона головы не более 10 градусов. Фотография должна быть резкой и контрастной. Как правило, комплексы позволяют на каждого человека заносить в базу данных любое количество фотографий. Лучшим вариантом является, когда лицо разыскиваемого находится на этих фотографиях в разных положениях.

В-пятых, комплекс должен быть интегрирован с программно-техническим комплексом «Розыск-Магистраль»¹⁶ и информационно-поисковыми системами органов внутренних дел.

Также необходимо обратить внимание на некоторые особенности применения комплексов биометрической идентификации.

Люди, идущие в потоке, могут смотреть как прямо перед собой, так и вправо или влево по ходу движения, а также опускать голову. Поэтому камеры биометрической видеофиксации необходимо размещать не под потолком, как камеры контроля за помещениями и периметром, а на уровне от 1 м 20 см до 1 м 50 см от уровня пола. Лучшей высотой является 1 м 30 см. Необходимо размещение видеокамер по обе стороны прохода.

Видеокамеры должны быть размещены на специальных опорах, выполненных в виде стоек ограждения, и быть защищены стандартным пылевлагозащищенным антивандальным корпусом. Это необходимо для их длительной бесперебойной работы. Возможна установка камер на стены или колонны при условии соблюдения высоты установки. В любом случае место установки камер должно быть огорожено, чтобы никто из пассажиров не мог стать напротив камеры, заслонив ее, и помешать идентификации идущих следом лиц.

Камеры должны быть установлены на расстоянии от 3 до 5 метров от точки фиксации. Как правило, точкой фиксации является выход из металлодетектора. Расстояние между камерами должно составлять 3-4 метра. При установке камер в метрополитене лучшим местом является их установка на стенах возле эскалатора. При выборе места размещения пункта прохода пассажиров следует учитывать, что все граждане, следующие через пост, должны гарантированно попасть в поле наблюдения видеокамер. Поле наблюдения имеет приблизительные размеры – 2 м ширины и 1,5 м высоты (нижний край поля наблюдения находится на расстоянии 1 м от пола).

Возможно расширение поля наблюдения или размещение камер на большем расстоянии. Однако для этого требуется или увеличение количества камер, или применение соответствующей расстоянию оптики. Для большей точности фиксации рекомендуется организация прохода наблюдаемого входа «в колонну по одному».

¹⁶ Приказ МВД России от 2 февраля 2008 г. № 100 «О внедрении программно-технического комплекса для доступа сотрудников уголовного розыска к АИС «Розыск-Магистраль». URL: <http://www.mvd.ru>

Для защиты камер от физических воздействий (толчков, ударов и т.п.) возможно также устанавливать мобильные ограждения (ленточные, стоечные и т.д.). Такое ограждение дополнительно сформирует поток и не позволит пассажирам случайно или намеренно миновать точку наблюдения.

В случае выявления в потоке разыскиваемого лица соответствующее сообщение передается на пост службы безопасности объекта и на рабочее место дежурного сотрудника ОВД (см. рис. 2.10), а также на носимое устройство оповещения ближайшему к месту выявления патрулю ППС, который может произвести необходимую проверку документов и другие соответствующие действия.



Рис. 2.10. Система распознавания лиц компании NtechLab

Таким образом, самое распространенное применение видеоаналитики – это охрана периметра. Причем любого – как полностью открытого, так и с забором и колючей проволокой. Это и любые границы, водные и сухопутные, полосы отчуждения, и просто открытые территории, куда посторонним вход ограничен. В поле зрения камеры, охраняющей периметр, можно очертить виртуальные линии – границы, при пересечении которых «правильными» объектами (т.е. не птицами и не кошками) будет выдано тревожное сообщение.

Также возможно создание зоны «отчуждения» – области перед охраняемыми границами, где, опять же, в зависимости от характеристик объекта и его поведения можем вызывать тревогу или можем потом использовать эту информацию для поиска объектов, проводивших подготовку нарушения. Достаточно эффективным инструментом является такая аналитика и для детектирования и поиска нарушений.

Кроме того, средства видеоаналитики позволяют обнаруживать оставленные или, наоборот, унесенные предметы, фиксировать траекторию движения объекта и даже отслеживать его перемещение от одной камеры к другой. Классификация объектов дает возможность понять, что именно движется в зоне наблюдения, их идентификация помогает определить степень угрозы, а распознавание ситуаций – выяснить, что же происходит на самом деле.

Как показывает статистика эксплуатации ПТК «Розыск-Магистраль», из каждых 25 тысяч пассажиров железнодорожного и воздушного транспорта средствами биометрической идентификации выявляется один человек, в отношении которого заведено розыскное дело, или человек, обоснованно подозреваемый в совершении преступлений, в отношении которого заведено оперативное дело.

В последние годы для защиты от террористической угрозы широко используются средства видеоаналитики. Их применение направлено на минимизацию человеческого фактора при поиске и слежении за подозрительными лицами и предметами, также на максимально эффективное «покрытие» всех охраняемых территорий.

При видеонаблюдении в залах аэропорта и на предприятиях, расположенных на его территории, системы видеоаналитики осуществляют распознавание лиц в толпе, обнаружение нетипичного поведения субъектов, отслеживание траектории выбранных субъектов, обнаружение оставленных предметов. Эти функции реализуются программно либо на уровне интегрированной системы безопасности, либо на уровне соответствующих подсистем.

Распознавание лиц часто используется при регистрации пассажиров на рейс. Математическая модель лица пассажира сравнивается с шаблонами, хранящимися в базе данных – БД (например, с базой лиц, находящихся в розыске). На рейс пассажир попадает в том случае, если совпадений с БД не обнаружено. Если же выясняется, что через пункт контроля намеревается пройти разыскиваемое лицо, организуется оповещение миграционных, таможенных служб, органов правопорядка. Подобная система может использоваться для автоматического сравнения фото в паспорте с «живым» лицом или для составления базы лиц, въезжающих в страну.

Производители камер видеонаблюдения идут по пути увеличения разрешения светочувствительных матриц и, если речь идет о купольной камере, то увеличения точности позиционирования и скорости поворотного механизма.

Это дает возможность при проектировании системы видеонаблюдения заложить минимальное количество камер, при этом автоматизировав процессы слежения в штатных ситуациях, запрограммировав варианты реакций на тревожные события, и реализовав в пользовательском интерфейсе возможности для наиболее удобного управления камерами (реальными или так называемыми «виртуальными», если мы имеем дело с панорамными камерами) и переключения с одной камеры на другую – например, с помощью графических планов.

При видеонаблюдении за большими открытыми площадями (например, за взлетно-посадочными полосами и рулежными дорожками) поворотные камеры часто используются в сочетании с детекторами движения. По мере передвижения самолета по взлетно-посадочной полосе, его текущее положение фиксиру-

ется детекторами движения, установленными вдоль ее края, индукционными петлями или другими датчиками. Сигналы с детекторов используются для управления поворотом камер видеонаблюдения, смонтированных вдоль другого края полосы. Таким образом, покрывается вся протяженность взлетно-посадочной полосы, что дает возможность отследить полностью процесс посадки или взлета самолета.

При использовании интеллектуальных детекторов движения важно решить проблемы отстройки от шумов и исключения ошибок, вызванных вибрацией камер под действием ветра, атмосферными явлениями, перемещением птиц и посторонних предметов в поле зрения камер. Проблема правильного обнаружения человека может быть решена экспериментальным путем.

Еще одна типовая задача, решаемая средствами видеонаблюдения – это контроль транспортных средств и распознавания номеров. Обязательному контролю подвергаются все транспортные средства, проезжающие на территорию аэропорта, причем контроль осуществляется круглосуточно. Система контроля проезда транспортных средств может быть взаимосвязана с системой паркинга.

Как правило, в составе такой системы выделяют две группы камер – обзорные и номерные. Обзорные камеры используются для ведения наблюдения за контрольно-пропускным пунктом и за территорией паркинга, а номерные камеры должны фиксировать государственные регистрационные номера автомобилей, въезжающих на территорию аэропорта и выезжающих с нее. Полученные кадры обрабатываются системой распознавания номеров, сверяются с базой данных и обязательно фиксируются. Если проезд транспортного средства на территорию аэропорта разрешен, то по сигналу разблокируется шлагбаум на въезде. Автоматически регистрируется время въезда и выезда каждого транспортного средства. Полученная информация может быть использована в системе документооборота аэропорта.

Видеонаблюдение позволяет эффективно решать многие задачи по обеспечению безопасности, однако по-настоящему эффективную систему безопасности такого объекта, как аэропорт, можно построить только путем тесной интеграции всех подсистем.

В аэропортах востребованы следующие функции видеоаналитики:

1. Детекция проникновения в запретные зоны.
2. Распознавание и фиксация лиц на точках входа на территорию или в здания аэропорта. В настоящее время аналитика распознавания лиц активно развивается, но пока не достигла достаточно высокой эффективности. Одна из причин – неполное количество информации о разыскиваемых нарушителях. Не секрет, что практически всем системам распознавания лиц для достижения высокой эффективности требуется «обучение». В большинстве случаев информация по разыскиваемым лицам представляет собой фотографии не самого высокого качества, но, тем не менее, системы уже довольно уверенно выдают похожие на разыскиваемых лица.

3. Распознавание и фиксация автомобильных номеров позволяет фиксировать время и место проезда автомобилей, строить автоматизированную систему пропуска автотранспорта на территорию и отслеживать логистику.

4. Детекция оставленных предметов помогает обращать внимание оператора на предметы, долгое время находящиеся на одном месте. Если для залов ожидания данная аналитика имеет мало смысла (так как здесь всегда долгое время без движения находится багаж), то места входов, кассовые залы и места проходов людей представляют большой интерес.

5. Детекция драк и нестандартного поведения позволяет обращать внимание операторов на подозрительные хаотичные и/или быстрые перемещения людей.

6. Детекция скопления людей – позволяет информировать о перегруженности отдельных зон, давая возможность быстро проанализировать причины и оперативно отреагировать (например, открыть дополнительные кассы или направить дополнительных сотрудников).

7. Детектор дыма – дополнительно к датчикам пожарной сигнализации позволяет обнаруживать задымления.

8. Детектор качества изображения – дает возможность фиксировать воздействие на сами камеры видеонаблюдения с целью их кражи или воспрепятствования проведению наблюдения за территорией.

Основные используемые модули видеоаналитики

Описание	Условия применения	Расположение камер	Возможности
Модуль интеллектуального детектора движения формирует метаданные с траекториями движения объектов и их укрупненные изображения	Везде		Обнаружение людей и транспортных средств в зоне наблюдения. Слежение за объектами в охраняемой зоне.
Модуль уличной видеоаналитики для обнаружения объектов неопределенной формы и тревожных ситуаций (сигнальная линия, движение в зоне, выявление всплесков и неравномерностей в движении, оставленный предмет), поддержка телевизионных и тепловизионных камер, отображение местоположения объекта (события) на плане территории	На улице или в больших помещениях	Высота установки – от 3 до 50 м Угол установки – не менее 15°	Охрана периметра. Обнаружение людей и транспортных средств в зоне наблюдения. Слежение за объектами в охраняемой зоне. Автоматическая классификация объектов на группы, например, человек, автомобиль не определен. Задание правил оперативного реагирования на объекты определенного типа.

Описание	Условия применения	Расположение камер	Возможности
Модуль видеоаналитики с детектором головы для потолочных камер и оживленных сцен (сигнальная линия, движение в зоне, оставленный предмет, движение против потока, скопление людей), отображение местоположения объекта (события) на плане территории	Везде	Минимальная высота установки – 2 м Рекомендуемая высота установки – 4-5 м. Угол установки – 90° (отклонение от горизонтали не менее 60°)	Подсчет и анализ поведения посетителей. Определение парного прохода через турникет. Сбор статистики и анализ данных.
Модуль распознавания государственных регистрационных знаков автомобилей	Только на улице	Высота установки – от 1,5 до 4,5 м Максимальный угол наклона видеокамеры: по вертикали – 30°; по горизонтали – 20°	Контроль присутствия и перемещения транспортных средств на территории любого размера. Создание видеоархива для быстрого и эффективного поиска нарушителей.
Модуль обнаружения скопления людей (толпы) на улице и внутри помещения	Везде	Высота установки – от 3 до 15 м. Угол установки – 5°-45°	Предупреждение правонарушений и массовых беспорядков на наблюдаемой территории. Срабатывает при превышении заданного порога количества людей в наблюдаемой зоне.
Модуль определения верхней части человека для детектирования людей на насыщенной сцене для их выделения из массы прочих объектов	Везде	Высота установки – от 3 до 50 м Угол установки – не менее 15°	Предупреждение правонарушений (праздношатание). Распознавание скоплений людей. Подсчет посетителей в очереди.
Модуль обнаружения, сопровождения лиц, выбора оптимального ракурса для формирования фотоальбома	Везде	Высота установки – чуть выше 2 м Угол установки – не более 5°	Отслеживание лиц в видеокадре в режиме реального времени и сохранение их в базу.
Модуль обнаружения резкого и быстрого движения, в том числе драки	Везде	Купольная камера. Угол установки – 90°	Отслеживание драк и потасовок в общественных местах в автоматическом режиме.
Модуль обнаружения дыма и огня	Только внутри помещения	Высота и угол установки произвольные, но поле зрения камеры не должно сильно перекрываться проходящими людьми и объектами	Раннее обнаружение пожара по изображению с камеры. Мониторинг больших производственных помещений.

Описание	Условия применения	Расположение камер	Возможности
Модуль контроля качества видео. Формирует события: нет сигнала, изображение слишком темное, слишком светлое, расфокусировано, содержит артефакты, частота кадров слишком низкая	Везде		Непрерывный контроль качества видеосигнала. Распознавание фактов несанкционированного вмешательства в работу интеллектуальной системы видеонаблюдения либо внезапного нарушения условий наблюдения.

На базе отдельных постов, установленных в аэропортах, появилась возможность создать общую территориально-распределенную систему видеонаблюдения и видеоаналитики. Преимущества такого «сотового» подхода заключаются в том, что архитектура системы организована по принципу конструктора: дополнительные видеокамеры и серверы добавляются в нее по мере необходимости и не влияют на работу других компонентов, то есть у них нет ограничений по числу подключаемых камер, серверов или рабочих мест.

Современные системы видеонаблюдения с возможностями видеоаналитики реагируют на преднамеренное закрытие камеры или засветку. Использовать обычные методы преступникам не удастся, поскольку общий контроль обстановки осуществляется в реальном времени, а детектирование нештатных ситуаций происходит в автоматическом режиме. Системы видеоаналитики могут отслеживать наличие дыма и огня, что крайне важно в помещениях с большим количеством людей и воспламеняющихся материалов.

Функциональные возможности систем видеоанализа позволяют отслеживать движение в зоне наблюдения. Детектировать оставленные и унесенные предметы, пересечение линии, вход/выход в зону/из зоны, отслеживать попытки прохода без билета или парного прохода через турникеты. Позволяют проводить анализ статистики локальных пассажиропотоков, что может быть использовано для разработки новых транспортных маршрутов и оптимизации существующих¹⁷.

К одному из уровней территориально-распределенной системы можно отнести и создание автоматизированных систем круглосуточного контроля въезда и выезда транспортных средств, хотя они могут работать и автономно на определенном объекте. Видеоаналитика позволяет распознавать номера автомобилей, автоматизировать пропускную систему, контролировать продолжительность и законность пребывания транспортных средств на парковке или охраняемой территории, анализировать данные о транспортных средствах, посетивших объект (место въезда/ выезда, дату, время и другие параметры). Позволяет назначать определенным транспортным средствам разные типы пропусков: постоянный, разовый, интервальный или кварталный.

¹⁷ Техника для спецслужб / Сайт компании «Бюро научно-технической информации». URL: <http://www.bnti.ru/>

Системы видеонаблюдения с функциями видеоаналитики позволяют фиксировать любую, а самое главное, неразрешенную активность вблизи и на стратегических объектах транспортной инфраструктуры страны. Они также помогают предотвратить внештатные ситуации, не связанные с террористической угрозой. Охранное видеонаблюдение не только дает качественную картинку с рубежей контроля, но и обеспечивает архивацию материалов, которые могут быть использованы для расследования тяжких преступлений, прежде всего террористических актов, т. е. системы осуществляют и ретроспективный анализ.

В зависимости от объекта при создании проекта системы видеонаблюдения учитываются особенности его расположения, назначение, условия эксплуатации. Кроме того, системы видеонаблюдения с элементами видеоаналитики позволяют анализировать происшествия и правильность действия персонала в той или иной критической ситуации.

В местах массового нахождения людей отслеживать их перемещение помогают системы дистанционной биометрической идентификации. Они способны сделать то, что простые системы видеонаблюдения и охранники сделать не в состоянии: за доли секунды выделить в толпе лицо человека и распознать его с достоверностью до 96%, сообщить на монитор охраны при совпадении с базой разыскиваемых лиц. Кроме того, системы могут определять пол и возраст проходящих через систему людей. Формирование баз лиц происходит непрерывно на всех объектах, где такие системы установлены.

Размещение систем дистанционного распознавания, например, в аэропортах, ускоряет процедуру прохождения паспортного контроля. С их помощью осуществляется пропуск в места с ограниченным доступом (СКУД). Возможна интеграция территориально распределенных систем видеонаблюдения с дистанционными системами биометрического распознавания, что позволяет сопоставлять данные обзорного видеонаблюдения и изображений лиц высокого разрешения в заданный временной промежуток с возможностью быстрого поиска необходимых видеоматериалов. С их помощью можно анализировать статистику локальных пассажиропотоков, детектировать нештатные ситуации: остановку движения пассажиропотока, «бегущего» человека, выявлять подозрительных лиц.

Большинство систем видеонаблюдения аэропорта обладают рядом ограниченных функций: просмотр, запись и быстрый поиск видеоряда. А интеллектуальные системы видеонаблюдения аэропорта позволяют значительно сэкономить на задействованном персонале службы безопасности и прочих системах. Но самое главное, они позволяют значительно снизить риски, связанные с умышленными и неумышленными действиями сотрудников и посторонних лиц.

Главное преимущество видеоаналитики перед обычными системами видеонаблюдения состоит в автоматическом выделении метаданных из потока видеоданных без участия оператора. Полученные метаданные могут быть использованы для быстрого поиска в видеоархиве, рассылки тревожных оповещений и сбора статистики.

В сравнении с «ручным видеонаблюдением», видеоаналитика позволяет уменьшить стоимость видеомониторинга и человеческого фактора в части обнаружения и времени реагирования.

Так как значительная часть видеоданных (более 99%) в системах видеонаблюдения не представляет интереса для пользователей, видеоаналитика позволяет кардинальным образом уменьшить нагрузку на каналы связи и систему архивирования за счет фильтрации ненужных видеоданных.

Приложения для анализа видеоданных не являются новинкой для индустрии систем видеонаблюдения. В России возможности видеоаналитики представлены российскими разработчиками программного обеспечения и мировыми производителями, представляющими свои камеры видеонаблюдения со встроенными возможностями видеоаналитики. Среди аналогов программного обеспечения на отечественном рынке можно встретить таких производителей, как «Интеллект», «Аххон Next», «Macroscop», «Линия». Каждый из производителей предлагает определенный набор интеллектуальных модулей.

Комплексный подход к формированию политики транспортной безопасности в масштабах государства и на каждом отдельном объекте, встраивание в системы видеонаблюдения алгоритмов видеоаналитики позволяет не только эффективно отслеживать нештатные ситуации, но и предупреждать их возникновение. Превентивные меры обеспечения безопасности транспортной инфраструктуры – вот главная задача систем видеонаблюдения на транспортных узлах и объектах.

Контрольные вопросы:

1. Охарактеризовать параметры камер видеонаблюдения.
2. Перечислить особенности формирования систем видеонаблюдения объектов аэропортовых комплексов.
3. Назвать особенности применения камер видеонаблюдения при обеспечении безопасности периметра аэропортового комплекса.
4. Перечислить требования к системе видеонаблюдения в здании аэровокзала.
5. Назвать возможности автоматизированных программно-аппаратных комплексов биометрической идентификации.
6. Перечислить необходимые условия функционирования системы видеоаналитики.
7. Описать возможности систем дистанционного распознавания лиц (предметов).
8. Перечислить требования к помещениям, из которых осуществляется управление инженерно-техническими системами и силами обеспечения транспортной безопасности.

ЗАКЛЮЧЕНИЕ

Популярность систем безопасности неуклонно растет. Уже не один десяток лет не ослабевает интерес к системам видеонаблюдения. Сегодня их используют не только на ответственных объектах коммерческого и общественного назначения, но и как элемент охранной инфраструктуры для частных нужд. Понимание того, какие виды и устройства камер видеонаблюдения предлагаются на современном рынке, позволит сделать правильный выбор, тем самым обеспечив надежную защиту. Модели устройств различаются по многим характеристикам, среди которых и качество «картинки», и возможности монтажа, и режимы эксплуатации.

Транспортная инфраструктура всегда была предметом особого внимания с точки зрения безопасности. Аэропорт лидирует по рискам среди всех остальных объектов транспортной инфраструктуры. Именно поэтому при организации системы видеонаблюдения в аэропорте необходимо тщательно выбирать решения для различных зон аэропортового комплекса, ведь по своей сути это целый город, которым управляют многочисленные аэропортовые службы.

Аэропорты склонны к террористическим нападениям, и поэтому строгий контроль является чрезвычайно важным в аэропортах. Системы видеонаблюдения помогают в борьбе с терроризмом и другими видами незаконной деятельности и облегчают работу правоохранительных органов в аэропортах. Видеонаблюдение в содействии с полной записью видеoinформации поддерживает высокий уровень безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности» (ред. от 06.07.2016) // Собрание законодательства Российской Федерации. 2007. № 7. Ст. 837.

2. Постановление Правительства Российской Федерации от 23.01.2016 № 29 «Об утверждении требований по обеспечению транспортной безопасности объектов транспортной инфраструктуры по видам транспорта на этапе их проектирования и строительства и требований по обеспечению транспортной безопасности объектов (зданий, строений, сооружений), не являющихся объектами транспортной инфраструктуры и расположенных на земельных участках, прилегающих к объектам транспортной инфраструктуры и отнесенных в соответствии с земельным законодательством Российской Федерации к охраняемым зонам земель транспорта, и о внесении изменений в Положение о составе разделов проектной документации и требованиях к их содержанию» // Собрание законодательства Российской Федерации. 2016. № 5. Ст. 698.

3. Постановление Правительства Российской Федерации от 01.02.2011 № 42 «Об утверждении Правил охраны аэропортов и объектов их инфраструктуры» (ред. от 17.12.2016) // Российская газета. 2011. № 25.

4. Распоряжение Правительства Российской Федерации от 15.05.2017 № 928-р «О перечне объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации» // Собрание законодательства Российской Федерации. 2017. № 21. Ст. 3065.

5. Приказ Минтранса России от 21.02.2011 № 62 «О Порядке установления количества категорий и критериев категорирования объектов транспортной инфраструктуры и транспортных средств компетентными органами в области обеспечения транспортной безопасности» (ред. от 10.10.2013) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2011. № 15.

6. Приказ Минтранса России от 08.02.2011 № 40 «Об утверждении Требований по обеспечению транспортной безопасности, учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств воздушного транспорта» (ред. от 10.10.2013) // Российская газета. 2011. № 54.

7. Приказ Минтранса России от 28.11.2005 № 142 «Об утверждении Федеральных авиационных правил "Требования авиационной безопасности к аэропортам"» (ред. от 24.05.2017) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2006. № 4.

8. ГОСТ Р 56461-2015 «Национальный стандарт Российской Федерации. Безопасность транспортная. Общие требования»: утв. и введен в действие Приказом Росстандарта от 15.06.2015 № 699-ст.

9. ГОСТ Р 51558-2014 «Национальный стандарт Российской Федерации. Средства и системы охраняемые телевизионные. Классификация. Общие техниче-

ские требования. Методы испытаний»: утв. и введен в действие Приказом Росстандарта от 22.10.2014 № 1371-ст.

10. ГОСТ Р 56875-2016 «Национальный стандарт Российской Федерации. Информационные технологии системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий»: утв. и введен в действие Приказом Росстандарта от 26.02.2016 № 81-ст.

11. ГОСТ 31817.1.1-2012 (ИЕС 60839-1-1:1988) «Межгосударственный стандарт. Системы тревожной сигнализации. Ч. 1. Общие требования. Раздел 1. Общие положения»: введен в действие Приказом Росстандарта от 22.11.2012 № 1034-ст.

12. ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Государственный стандарт Российской Федерации. Системы тревожной сигнализации. Ч. 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию»: принят и введен в действие Постановлением Госстандарта РФ от 22.05.1995 № 256 (ред. от 13.12.2011).

13. Р 78.36.018-2011 «Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности»: утв. МВД России 20.12.2011.

14. Р 78.36.002-2010 «Рекомендации. Выбор и применение систем охраняемых телевизионных»: утв. МВД России 07.05.2010.

15. Р 78.36.039-2014 «Рекомендации. Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения».

16. Р 78.36.029-2014 «Об оснащении ПЦО средствами аудио- и видеонаблюдения. Методические рекомендации».

17. Котельников А.В. Программные средства, предназначенные для расчетов параметров систем охранного телевидения // Научно-технический портал МВД России. 2014. №1(9).

18. Статья «видеоаналитика: материал из свободной энциклопедии Википедия. URL: <https://ru.wikipedia.org/wiki>.

19. Особенности использования информационных технологий в органах внутренних дел на транспорте: учебное пособие / И.Ф. Амельчаков, П.Н. Жукова, А.Н. Прокопенко [и др.]. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2016. – 118 с.

20. Жукова П.Н., Насонова В.А., Прокопенко А.Н. Обеспечение безопасности на объектах транспортной инфраструктуры посредством использования систем видеонаблюдения и видеоаналитики // Проблемы правоохранительной деятельности. 2015. № 4. С. 91-96.

21. Жукова П.Н., Насонова В.А., Прокопенко А.Н. Возможности использования информационных технологий при борьбе с организованной преступностью на объектах транспортной инфраструктуры / Математические методы и информационно-технические средства: материалы XII Всероссийской научно-практической конференции (Краснодар, 17 июня 2016 г.). – Краснодар: Краснодарский университет МВД России, 2016. С. 105-109.

Принятые сокращения

АДИС – автоматизированная дактилоскопическая информационная система.
АНВ – акт незаконного вмешательства.
АПКБИ – автоматизированные программно-аппаратные комплексы биометрической идентификации.
АРД – автоматическая регулировка диафрагмы камеры.
АРМ – автоматизированное рабочее место.
ГЛОНАСС – Глобальная навигационная спутниковая система.
ГУТ МВД России – главное управление на транспорте МВД России.
ЕГИС ОТБ – единая государственная информационная система обеспечения транспортной безопасности.
ИДК – инспекционно-досмотровый комплекс.
ИМТС – интегрированная мультисервисная телекоммуникационная система.
ИСОД МВД России – единая система информационно-аналитического обеспечения деятельности МВД России.
ИТС – интеллектуальные транспортные системы.
КПК – карманный персональный компьютер.
КПП – контрольно-пропускной пункт.
ЛО – линейный отдел.
ЛУ – линейное управление.
МВД – министерство внутренних дел.
ОАО «РЖД» – открытое акционерное общество «Российские железные дороги».
ОПГ – организованная преступная группировка.
ОТИ – объекты транспортной инфраструктуры.
ПК – персональный компьютер.
ПТК «Розыск-магистраль» – программно-технический комплекс «Розыск-магистраль».
ПО – программное обеспечение.
ПЦО – пункт централизованной охраны.
САБ – служба авиационной безопасности.
САВП – системы автоматизированного ведения поездов.
СКУД – система контроля доступа.
СУДИС – система управления доступом к информационным системам и ресурсам.
ТС – транспортное средство.
ТУ – телеуправление.
ФСБ – Федеральная служба безопасности.
ЦДП – центральный диспетчерский пункт объекта транспортной инфраструктуры.
ЦОД – центр обработки данных.
ЭВМ – электронно-вычислительная машина.

УЧЕБНОЕ ИЗДАНИЕ

Жукова Полина Николаевна,
доктор физико-математических наук, доцент;
Прокопенко Алексей Николаевич,
кандидат технических наук, доцент;
Насонова Валентина Афанасьевна,
кандидат физико-математических наук, доцент;
Дрога Андрей Анатольевич;
Гуржий Алексей Александрович

**Использование систем видеонаблюдения и видеоаналитики
для обеспечения безопасности на объектах транспортной инфраструктуры (аэропорты)**

Учебное пособие

Редактор
Комп. верстка

О.Н. Тулина
И.Ю. Чернышева

Подписано в печать 22.06.2018, 4,5 уч.-изд. л., бумага офсетная, печать трафаретная.
Тираж 52 экз. Заказ № 24

Отпечатано в отделении полиграфической и оперативной печати
Белгородского юридического института МВД России имени И.Д. Путилина
г. Белгород, ул. Горького, 71

ISBN 978-5-91776-225-8



9 785917 762258