Видеонаблюдение в музее

Руководство

(Методические рекомендации)

2023

ВИДЕОНАБЛЮДЕНИЕ В МУЗЕЕ

Руководство
(Методические рекомендации)

Научный редактор:
Богданов Алексей Валентинович,
к.т.н., доцент, заместитель генерального директора ФГБУК «Государственный Эрмитаж»

Авторы:
Райников Александр Вадимович
(ФГБУК «Государственный Эрмитаж»)

Ульянов Олег Андреевич
(эксперт Ассоциации «Безопасность туризма»
в сфере видеонаблюдения)

Мануйлов Иван Сергеевич
(эксперт Ассоциации «Безопасность туризма»
в сфере видеонаблюдения, ООО «НЕКСТ»)

Донцов Николай Юрьевич
(ФГБУК «Государственный Русский музей»)

2023

Цель разработки настоящего Руководства (Методических рекомендаций) – содействие руководителям и иным должностным лицам музеев в решении задач и соблюдении процедур при выполнении обязательных требований Единых правил организации комплектования, учета, хранения и использования музейных предметов и музейных коллекций (утв. приказом Министерства культуры Российской Федерации от 27 июля 2020 года № 827, далее – Единые правила).

Одним из требований Единых правил является обеспечение охранного режима и эффективной контрольно-пропускной системы и охранного телевидения.

В Руководстве (Методических рекомендациях) приведены и использованы примеры и передовые практики отдельных музеев по организации соблюдения обязательных требований Единых правил в части охранного видеонаблюдения. Руководство (Методические рекомендации) подготовлены в соответствии со ст. 14 Федерального закона от 31 июля 2020 года № 247-ФЗ «Об обязательных требованиях в Российской Федерации».

В Руководстве (Методических рекомендациях) не содержатся новые обязательные требования, оно носит рекомендательный характер. За невыполнение Руководства (Методических рекомендаций) меры административного воздействия не применяются.

Руководство (Методические рекомендации):

- содержит основные принципы организации и эксплуатации систем видеонаблюдения с учетом специфики вопросов музейной безопасности;
- включает информацию, необходимую при проектировании и настройке современных систем видеонаблюдения, могут являться инструментом для взаимодействия с подрядными организациями;
- содержит типовые требования к элементам систем видеонаблюдения и местам размещения оборудования;
- предназначено для руководителей и заместителей руководителей по безопасности и инженерно-техническим вопросам, руководителей и сотрудников служб безопасности учреждений в соответствии с Едиными правилами организации комплектования, учета, хранения и использования музейных предметов и музейных коллекций, утвержденными приказом Минкультуры России от 23 июля 2020 года № 827.

Разработано по решению:

Экспертно-технического совета при Межведомственной рабочей группе по выработке предложений, связанных с обеспечением охраны музейных предметов и безопасности в музеях Российской Федерации.

При участии:

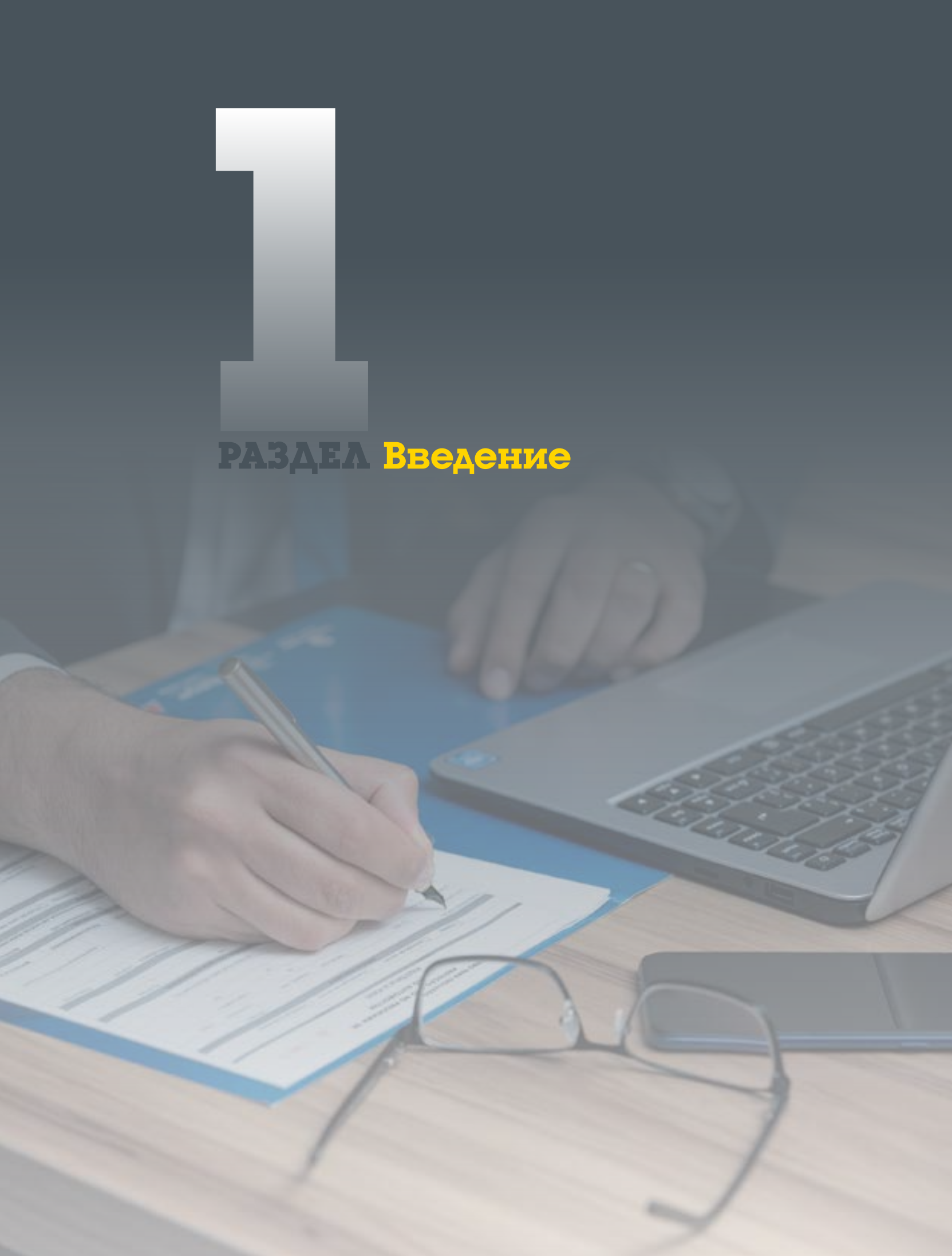
- Российского комитета Международного совета музеев (ИКОМ России);
- ФГБУК «Государственный Эрмитаж»;
- ФГБУК «Всероссийское музейное объединение «Государственная Третьяковская галерея»;
- ФГБУК «Политехнический музей»;
- ФГБУК «Государственный Русский музей»;
- ГБУК г. Москвы «Мосразвитие»;
- Союза музеев России;
- Комитета по безопасности объектов культуры и культурного наследия Ассоциации «Безопасность туризма»;
- Волхонского Владимира Владимировича (Университет ИТМО).

Содержание

Наименования глав и приложения содержат активные ссылки на соответствующие страницы Рекомендаций

1

РАЗДЕЛ Введение



Основной целью настоящих Методических рекомендаций «Система видеонаблюдения» (далее – МР) является создание универсального инструмента для помощи руководителям музейных учреждений, руководителям и специалистам служб безопасности музейных учреждений, музейным хранителям, руководителям и специалистам служб инженерной эксплуатации музейных учреждений в решении следующих задач:

- определение порядка и особенностей организации и эксплуатации системы видеонаблюдения музейного учреждения;
- применение систем видеонаблюдения в составе комплексной интегрированной системы безопасности;
- выбор характеристик оборудования для системы видеонаблюдения;
- выбор мест установки видеокамер и мест размещения вспомогательного оборудования;
- организация диспетчерского пульта.

В связи с недостаточным наполнением нормативно-правовой базы в области систем видеонаблюдения при создании МР принимались за основу требования, предъявляемые к современным системам видеонаблюдения с учетом специфики обеспечения безопасности музейных учреждений. МР рекомендованы к изучению руководителям и сотрудникам музейных учреждений, деятельность которых связана с организацией безопасности учреждения и сохранности музейных предметов.

Содержание МР наглядно представлено **в главе 5.1** на общей структурной схеме типовой системы видеонаблюдения. Схема содержит ссылки на главы, в которых указана подробная информация по структурным элементам систем.

Методические рекомендации разбиты на следующие основные разделы:

1. Введение.
2. Термины и определения.
3. Задачи систем видеонаблюдения на объектах культуры.
4. Нормативное регулирование.
5. Общая структура систем видеонаблюдения.
6. Эксплуатационные требования к качеству изображения для решения поставленных задач.
7. Основы выбора количества и мест размещения видеокамер и других элементов системы видеонаблюдения.
8. Типовые решения по реализации видеонаблюдения для различных категорий объектов.
9. Основы построения сети передачи данных, системы сбора, обработки и хранения информации.
10. Программное обеспечение систем видеонаблюдения и особенности его лицензирования.
11. Принципы интеграции с подсистемами обеспечения безопасности, автоматизации здания и иными информационными системами.
12. Принципы организации диспетчерского пульта видеонаблюдения.
13. Видео- и аудиоаналитика.
14. Особенности технического обслуживания, эксплуатации и проектирования.
15. Оценка целесообразности и выбор метода резервирования вычислительных устройств.
16. Основы расчета параметров системы хранения данных для системы видеонаблюдения.
17. Приложение.

Изложение материала в МР дается комплексно, для формирования полного представления о принципах организации системы видеонаблюдения музейного учреждения.

В первой части МР представлены основные положения для постановки задач, которые способна решать система видеонаблюдения, перечислены нормативные документы, устанавливающие требования в части организации систем охранного телевидения на объектах культуры и в местах массового пребывания людей.

Глава 5.2 «Эксплуатационные требования к качеству изображения для решения поставленных задач» содержит информацию об основных характеристиках, которым должно соответствовать изображение, получаемое с видеокамер в целях мониторинга, обнаружения, наблюдения, распознавания и идентификации объектов.

Основные рекомендации по местам размещения, функциональному назначению и характеристикам видеокамер представлены в таблице № 4 **главы 5.3.** Перечень содержит требования к качеству изображения с рекомендациями по эффективному использованию ресурсов систем видеонаблюдения. Следующая глава содержит образец типового объекта с учетом рекомендаций, указанных в **главе 5.3.** На плане объекта указаны основные места использования видеокамер с указанием зон охвата.

Последующие части МР состоят из глав, содержащих детальное описание компонентов, на основе которых создается любая система видеонаблюдения:

- сеть передачи данных;
- система хранения данных;
- программное обеспечение (включая особенности лицензирования);
- видеоаналитика.

Отдельные главы посвящены принципам создания единой интегрированной системы безопасности с примерами эффективных алгоритмов взаимодействия между подсистемами, основам организации диспетчерского пульта для операторов видеонаблюдения, а также особенностям технического обслуживания и эксплуатации, включая требования по организации серверных помещений.

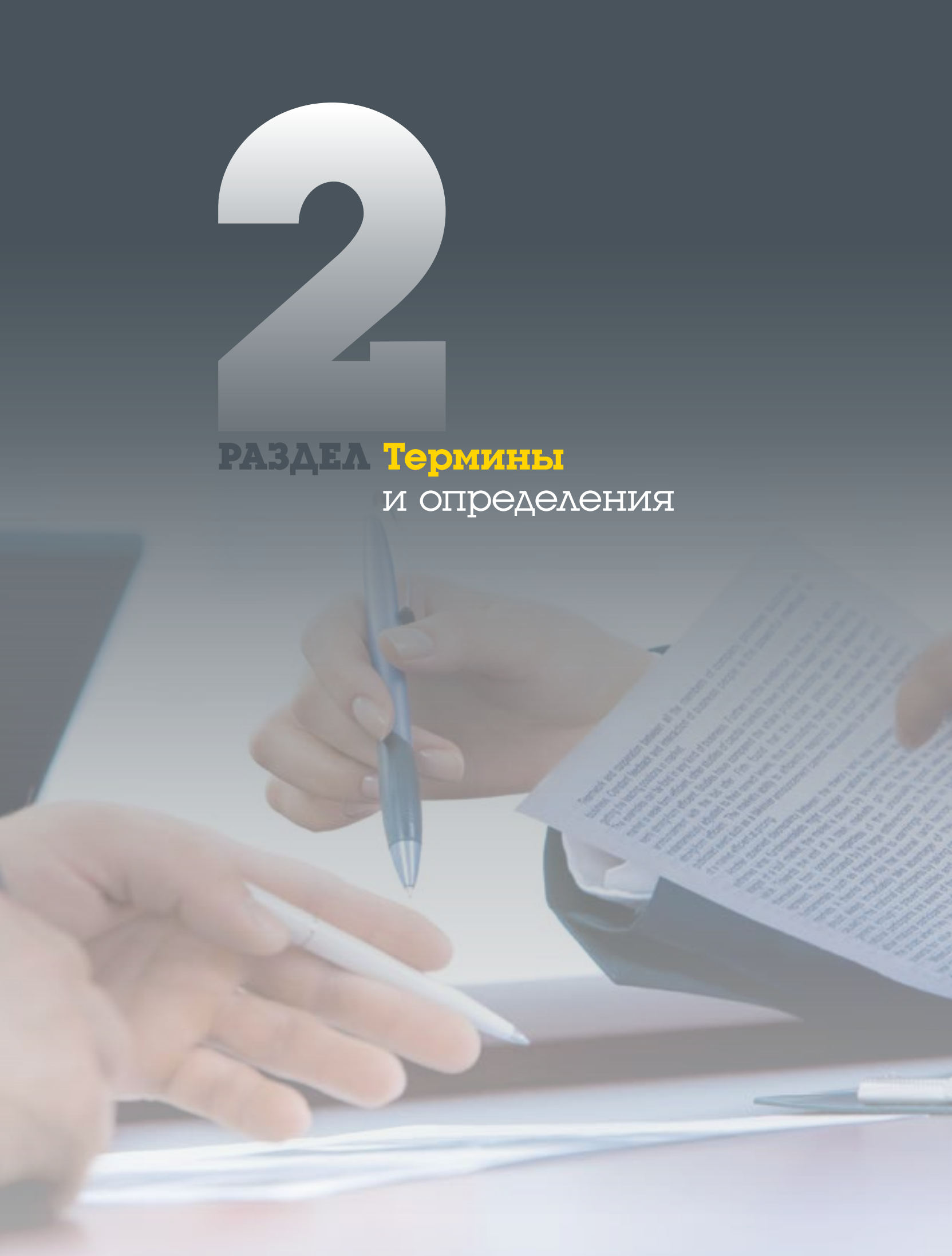
Оценки технологических ресурсов систем видеонаблюдения представлены в **главах 6.1** и **6.2**. Данные материалы служат инструментом для анализа эффективности работы системы, позволяют произвести ориентировочные расчеты параметров системы хранения данных и заложить необходимый резерв оборудования.

В состав **Приложения** включен типовой регламент технического обслуживания системы видеонаблюдения.

На этой странице текст зеленого цвета содержит гиперссылку

2

РАЗДЕЛ Термины и определения

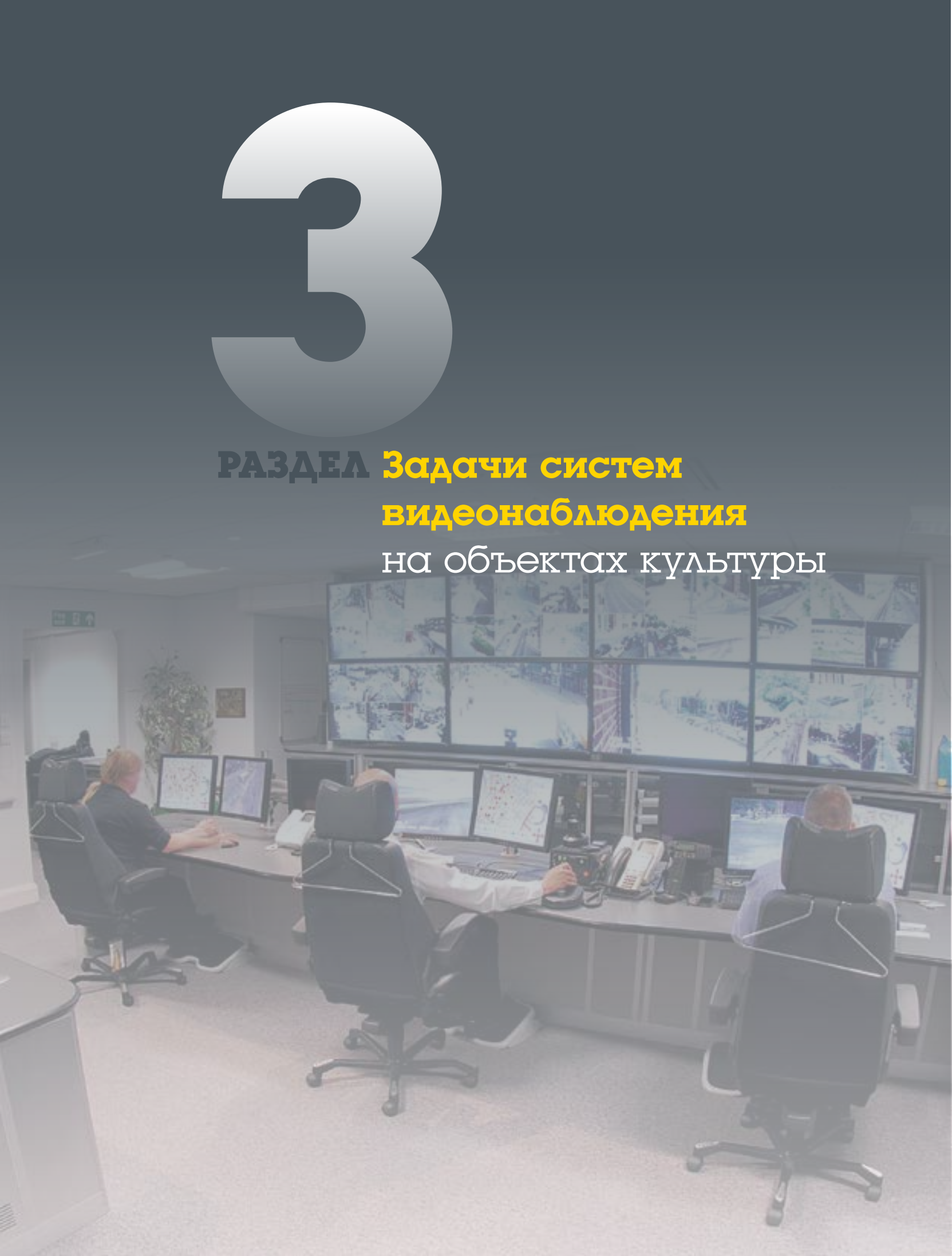


ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

СОТ – система охранного телевидения.
ЛВС (LAN) – локальная вычислительная сеть.
ТСБ – телевизионные системы безопасности.
СХД – системы хранения данных.
NAS (Network Attached Storage) – является сервером для хранения данных на файловом уровне. По сути, представляет собой компьютер с некоторым дисковым массивом, подключенный к сети (обычно локальной) и поддерживающий работу по принятым в ней протоколам. Несколько таких компьютеров могут быть объединены в одну систему.
JBOD (англ. Just a Bunch of Disks – «просто пачка дисков») – дисковый массив, в котором единое логическое пространство распределено по жестким дискам последовательно.
NVR (Network Video Recorder) – специализированное устройство, предназначенное для записи видеоизображения с IP-видеокамер, подключенных как к сети ЛВС, так и напрямую к NVR (NVR со встроенными коммутаторами).

3

РАЗДЕЛ Задачи систем видеонаблюдения на объектах культуры



Человек получает не менее 60 % всей информации о внешнем мире при помощи зрения. Данный факт крайне важен при рассмотрении вопросов комплексной безопасности объекта. Возможность визуального подтверждения сообщений о тревоге позволяет повысить эффективность работы персонала и сократить время принятия решения при возникновении нештатной ситуации. Основным средством обеспечения визуального подтверждения события в удаленной точке объекта охраны является система видеонаблюдения.

Основная функция системы видеонаблюдения – дистанционное наблюдение за объектом в определенной области с возможностью сбора, обработки и хранения видеоданных, включая последующий просмотр и анализ.

Задачи, которые решаются на объектах культуры при помощи систем видеонаблюдения, давно вышли за рамки только охранного телевидения. Видеонаблюдение применяется для решения многих вопросов обеспечения комплексной безопасности в сочетании с другими подсистемами.

СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ ПРИМЕНЯЕТСЯ ПРИ РЕШЕНИИ СЛЕДУЮЩИХ ЗАДАЧ:

Мониторинг – передача общей картины происходящего на объекте в реальном времени для принятия планомерных организационных решений персоналом.

Охрана правопорядка и предотвращение нарушений – своевременное автоматическое обнаружение нарушений режима объекта и/или автоматическое представление вспомогательной информации по сигналам от ТСБ объекта, дальнейшее сопровождение реакции на событие, в том числе помощь в локализации и задержании нарушителя средствами видеоаналитики.

Идентификация объектов – идентификация людей, транспортных средств в целях подтверждения прав доступа в определенную зону.

Анализ происшествий и проведение расследований (формирование доказательной базы для разбора инцидентов) – просмотр и анализ видеоданных, записанных в архив.

Сбор статистической, маркетинговой и иной вспомогательной информации средствами видеоаналитики – данные о количестве посетителей, очередях, скоплении людей, наиболее популярных местах посещения, данные с кассовых аппаратов и т. д.

Контроль и оценка ситуации в местах с ограниченным постоянным присутствием человека – технические помещения, отдельные части опасных производственных объектов.

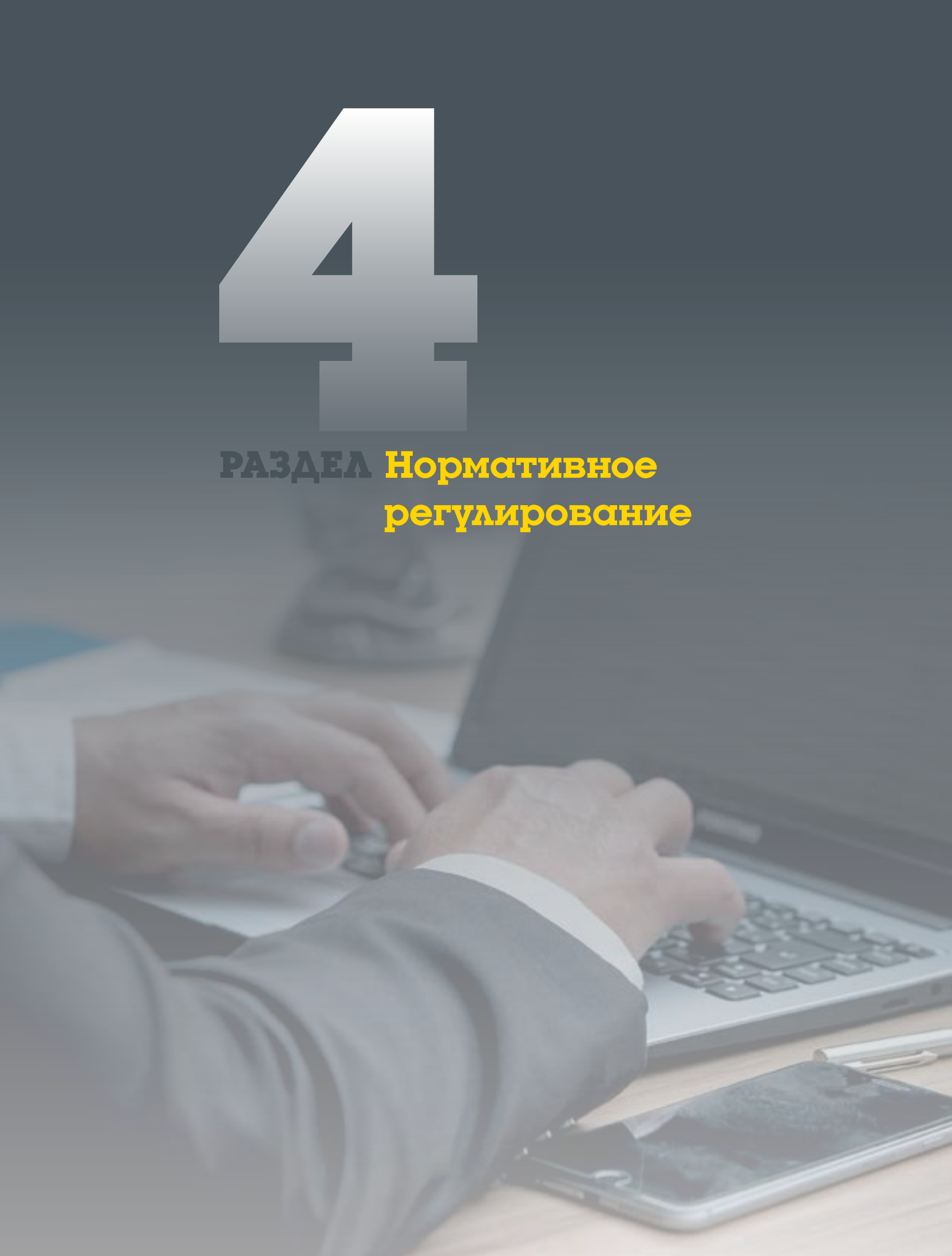
Входной контроль температуры персонала и посетителей – обеспечение эпидемиологической безопасности.

ПРИМЕЧАНИЕ: *Перечень задач не является исчерпывающим, возможности применения наблюдения зависят от особенностей каждого конкретного объекта.*

Система видеонаблюдения способна эффективно решать указанные задачи при условии соответствия определенным требованиям к информативности видеоизображения при различных внешних факторах. Современное оборудование позволяет в кратчайшие сроки организовать наблюдение при низкой освещенности, при полном отсутствии освещения (ИК-подсветка), на большом расстоянии (использование телеобъективов) и так далее. Видеоаналитика на сегодняшний день является неотъемлемой частью систем видеонаблюдения и будет приниматься в данных методических рекомендациях по умолчанию в качестве стандартной функции, присутствующей в видеокамерах.

4

РАЗДЕЛ Нормативное регулирование



В таблице № 1 перечислены нормативные документы, устанавливающие требования к системам охранного телевидения, в том числе в сфере культуры и в местах массового пребывания людей.

Таблица № 1

Нормативный документ	Описание
ГОСТ Р 51558-2014. Национальный стандарт Российской Федерации. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний	Настоящий стандарт распространяется на вновь разрабатываемые и модернизируемые системы охранные телевизионные и технические средства в составе СОТ, предназначенные для получения аудио- и (или) видеоинформации с охраняемого объекта в целях обеспечения противокриминальной защиты.
Гражданский кодекс РФ	В части взаимоотношений с гражданами при организации видеонаблюдения.
Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»	Определяет порядок получения, обработки, хранения персональных данных.
Постановление Правительства РФ от 25 марта 2015 года № 272	«Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий)» (с изм. и доп., вступ. в силу с 10.10.2020), пункты 37–40, 52.
Постановление Правительства РФ от 11 февраля 2017 года № 176	«Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий)», пункт 27 (а).
Постановление Правительства РФ от 05 марта 2021 года № 331	Постановление устанавливает обязанность по формированию и ведению информационной модели объекта капитального строительства в случае, если договор о подготовке проектной документации для строительства, реконструкции объекта капитального строительства, финансируемых с привлечением средств бюджетов бюджетной системы Российской Федерации, заключен после 1 января 2022 года, за исключением объектов капитального строительства, которые создаются в интересах обороны и безопасности государства.
Приказ Министерства культуры РФ от 08 ноября 2000 года № 664	Утверждает типовые требования по инженерно-технической укрепленности и оборудованию техническими средствами охраны учреждений культуры, расположенных в зданиях – памятниках истории и культуры.
РД 78.36.002-2010	Рекомендации «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения» (утв. МВД РФ 15 апреля 2010 года).

На этой странице текст зеленого цвета содержит гиперссылку

5

РАЗДЕЛ Основные принципы организации и эффективной эксплуатации

Данная глава посвящена подробному описанию основ построения систем видеонаблюдения с указанием рекомендаций по эффективному использованию главных элементов системы.

ГЛАВА 5.1. ОБЩАЯ СТРУКТУРА СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

Системы видеонаблюдения являются совокупностью множества устройств и программно-аппаратных средств, выполняющих различные функции. На **рис. 1** представлена обобщенная структурная схема типовой системы видеонаблюдения. Схема содержит ссылки на отдельные главы методических рекомендаций, посвященные отдельным вопросам по организации и эффективной эксплуатации элементов комплексной системы безопасности.

ВЫВОД: *Системы видеонаблюдения построены на базе обобщенной структуры, включающей источники видеосигнала, каналы связи, устройства обработки и хранения, устройства отображения, а также средства видеоаналитики и средства интеграции с иными подсистемами.*

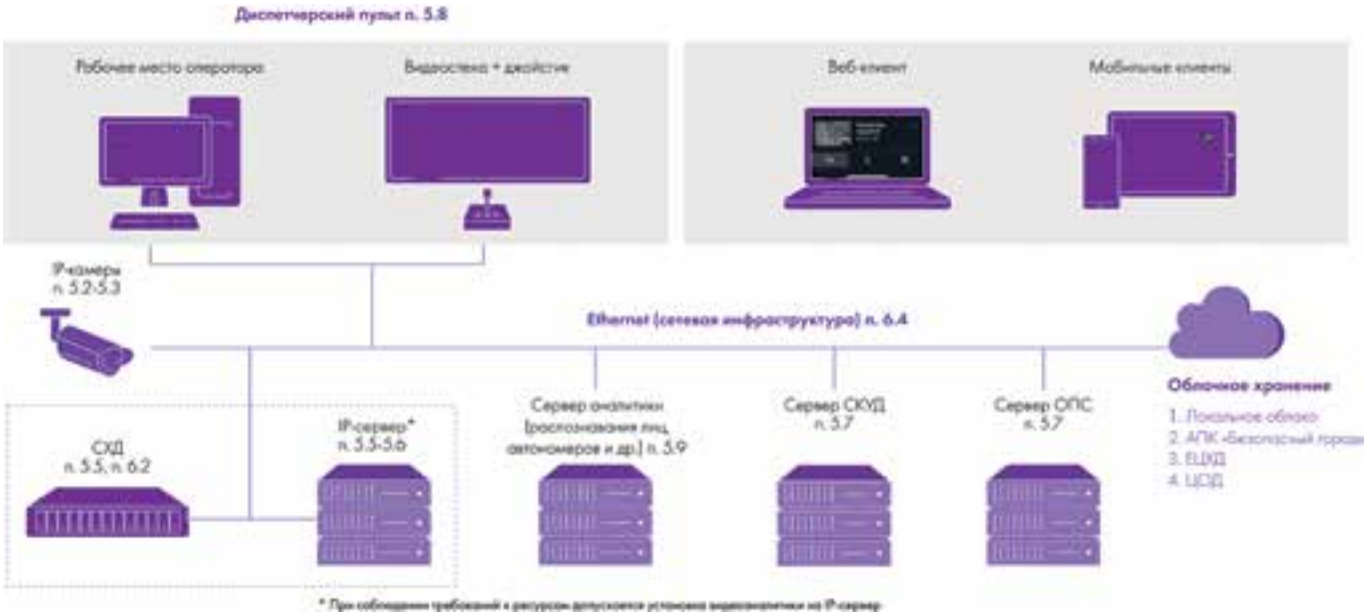


Рис. 1. Структурная схема системы видеонаблюдения

ГЛАВА 5.2. ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ К КАЧЕСТВУ ИЗОБРАЖЕНИЯ ДЛЯ РЕШЕНИЯ ПОСТАВЛЕННЫХ ЗАДАЧ

Способность различать объекты на больших и малых расстояниях является одной из важнейших характеристик, влияющих на эффективность системы видеонаблюдения. Независимо от используемых технологий основным инструментом оператора является изображение или поток кадров, формируемые видеокамерой. Качество изображения, получаемого с видеокамеры, должно соответствовать определенным требованиям в зависимости от задачи, поставленной перед оператором для установленной зоны наблюдения. Рассмотрим перечень задач, которые может решать оператор при просмотре изображения с видеокамер (**таблица № 2**).

Для решения описанных задач группами экспертов и производителей оборудования определены требования к характеристикам просматриваемого изображения. До повсеместного внедрения цифровых видеокамер главным параметром определения качества изображения на соответствие той или иной задаче являлся показатель величины процента от высоты экрана (при условии соответствия разрешения монитора и видеокамеры), занимаемой объектом интереса.

С развитием цифровых стандартов видеоизображения основополагающей величиной для решения поставленных перед оператором задач является плотность пикселей, то есть количество пикселей на единицу физического размера объекта интереса (**таблица № 3**).

Значение плотности пикселей зависит от разрешающей способности камеры, от расстояния от камеры до объекта интереса и от угла обзора телекамеры. Увеличение максимального разрешения видеокамеры позволяет увеличить плотность пикселей в области наблюдения и, соответственно, обеспечить лучшее качество детализации. Кроме того, чем бóльшую площадь изображения занимает какой-либо объект, тем большее количество пикселей в нем содержится, а следователь-

На этой странице текст зеленого цвета содержит гиперссылку

Таблица № 2

Задача	Описание
Мониторинг	Эта область предназначена для наблюдения за транспортным потоком или за движением людей без необходимости различения отдельных фигур на обширной территории.
Обнаружение	Уровень детализации в этой области позволяет гарантированно определить присутствие человека в кадре.
Наблюдение	В этой области могут быть видны некоторые характерные детали, такие как предметы одежды, при этом сохраняется широкий обзор для отслеживания действий вокруг.
Распознавание	В данной области оператор способен определить, знаком или неизвестен распознанный человек.
Идентификация (благоприятные/сложные условия)	Качество и детализация изображения должны быть достаточными для того, чтобы личность человека могла быть установлена с высокой степенью вероятности. В связи с различными внешними факторами в месте установки видеокамеры зону идентификации разделяют в зависимости от окружающих условий: ■ благоприятные – наблюдаемые объекты передвигаются с умеренной скоростью, мелкие детали, необходимые для распознавания, хорошо видны в кадре, освещение достаточное для получения качественной картинки; ■ сложные – уровень освещения недостаточен или значительно меняется в короткий промежуток времени, наблюдаемые объекты передвигаются с большой скоростью, либо видны под углом, в результате часть деталей оказывается вне поля зрения камеры.
Инспектирование	В этой области происходит 100-процентная идентификация, исключающая сомнения. Данная зона применима в отдельных случаях и требует установки отдельной категории оборудования.

Таблица № 3

	Величина процентов от высоты экрана		Плотность пикселей		Вспомогательные характеристики	
	Проценты от высоты экрана для стандарта, PAL	Проценты от высоты экрана для разрешения, 1080p	мм/пикс	пикс/м	Минимальное кол-во пикселей на ширину лица	Максимальная ширина сцены для камеры с разрешением Full HD, м
Мониторинг	5	2	80	12,5	2	153,6
Обнаружение	10	4	40	25	4	76,8
Наблюдение	25–30	10	16	62,5	10	30,72
Распознавание	50	19	8	125	20	15,36
Идентификация благопр.	100	38	4	250	40	7,68
Идентификация неблагопр.	–	–	2	500	80	3,84
Инспектирование	400	152	1	1000	160	1,92

но, более мелкие детали объекта различимы для нашего глаза.

Для выбора нужного разрешения камеры необходимы формулировка задачи наблюдения, определяющая требуемую плотность пикселей (табл. 3), расстояние от камеры в дальней части зоны наблюдения, в которой должна решаться задача наблюдения и угол обзора. Только после выбора плотности пикселей, расстояния от камеры и угла обзора можно правильно выбрать разрешение.

ВАЖНО! ***Нужно внимательно относиться к выбору конкретного решения, иногда вариант установки нескольких видеокамер с более низкой разрешающей способностью будет существенно эффективнее, чем одна видеокамера с высокой.***

Величина процентов от высоты экрана и плотность пикселей взаимосвязаны и позволяют рассчитать вспомогательные характеристики, необходимые при проектировании систем видеонаблюдения, такие как минимальное количество пикселей на ширину лица (стандартная ширина лица человека – 16 см) и максимальную ширину сцены для каждой зоны.

Показатели, указанные в таблице №3, являются усредненными значениями для различных типов видеокамер и внешних условий размещения видеокамер. Из этого не следует, что будет невозможно распознать или идентифицировать человека, если размер изображения меньше, чем предложенные 50 % или 125 пикс/м. Точно так же нет никакой гарантии, что отдельные лица будут идентифицированы только потому, что они занимают менее 100 % экрана. Как упоминалось ранее, помимо показателя плотности пикселей, существует ряд факторов, оказывающих влияние на качество изображения.

К таким факторам относятся:

- освещенность – величина освещенности должна соответствовать уровню чувствительности, указанному в характеристике видеокамеры (дневной/ночной режимы);
- глубина резкости – должна покрывать всю зону контроля, объекты должны быть различимы;
- высота установки, угол наклона камеры, фокусное расстояние объектива камеры – данные показатели должны соответствовать поставленной задаче. Вероятность правильной идентификации напрямую зависит от высоты установки видеокамеры и угла наклона. В частности, для идентификации лиц камера должна быть установлена с отклонением центральной оси наблюдения не более 15 градусов;
- угол разворота лица, скорость перемещения объекта – показатели, влияющие на решение задач распознавания, идентификации и инспектирования. При решении данных задач рекомендуется устанавливать видеокамеру так, чтобы человек находился лицом к видеокамере и угол разворота был минимальным. Выбор зоны обзора видеокамеры должен производиться с учетом скорости перемещения объектов и захватывать максимальную длину пути объекта в кадре.

ПРИМЕЧАНИЕ: *Необходимо различать понятия плотности пикселей на изображении (на единицу длины) и плотность пикселей на матрице видеокамеры (технологический параметр). Отметим, увеличение плотности пикселей на фиксированном размере матрицы видеокамеры приводит к общему снижению чувствительности матрицы, и, как следствие, в неблагоприятных условиях съемки получаемое изображение может иметь существенно более низкое качество («мыльность», «шумы»).*

Для проектирования и проверки соответствия заданным требованиям в системах видеонаблюдения существует ряд вспомогательных программ. Такие инструменты позволяют увидеть, в каких частях зоны обзора камеры обеспечивается достаточная разрешающая способность для идентификации, распознавания, наблюдения, обзора и мониторинга различных объектов видеонаблюдения, в частности людей и машин.

Использование трехмерного изображения позволяет отображать картинку с видеокамер в режиме виртуальной реальности с настройкой угла поля зрения и параметров разрешения видеокамер в модели с учетом слепых зон.

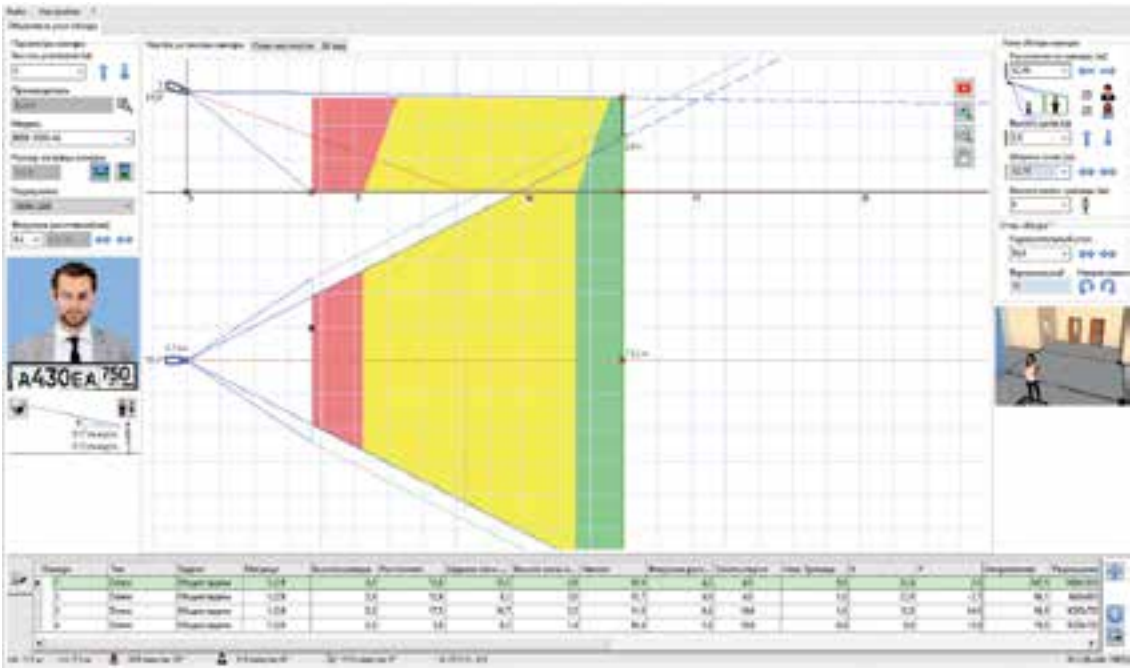


Рис. 2. Чертеж установки видеокамеры

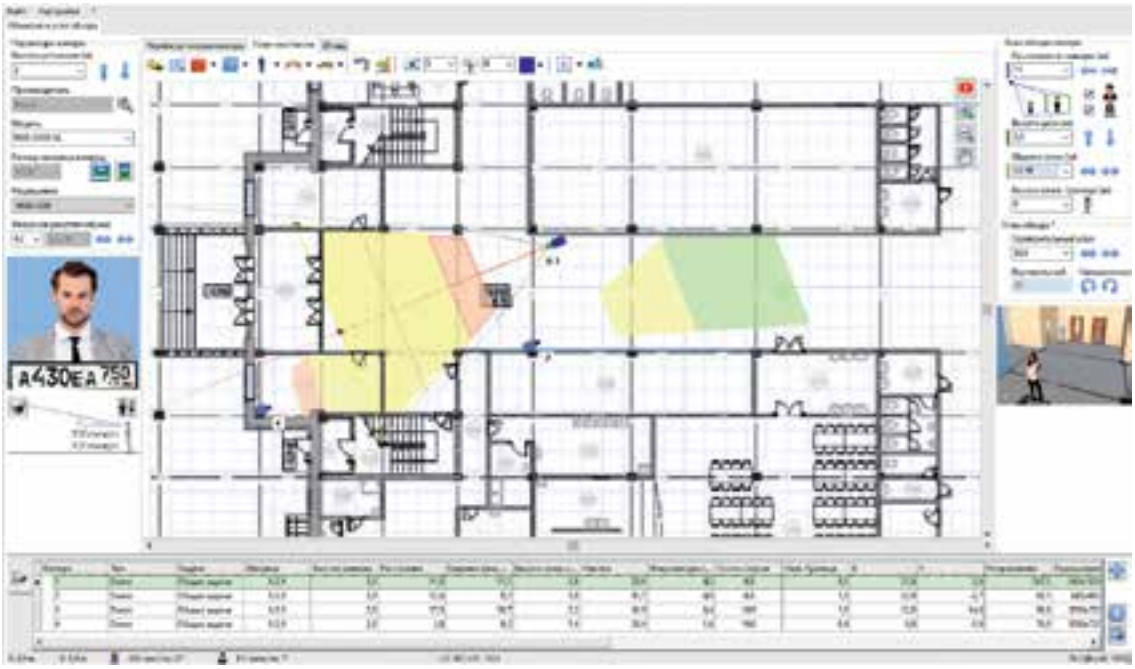


Рис. 3.
План местности

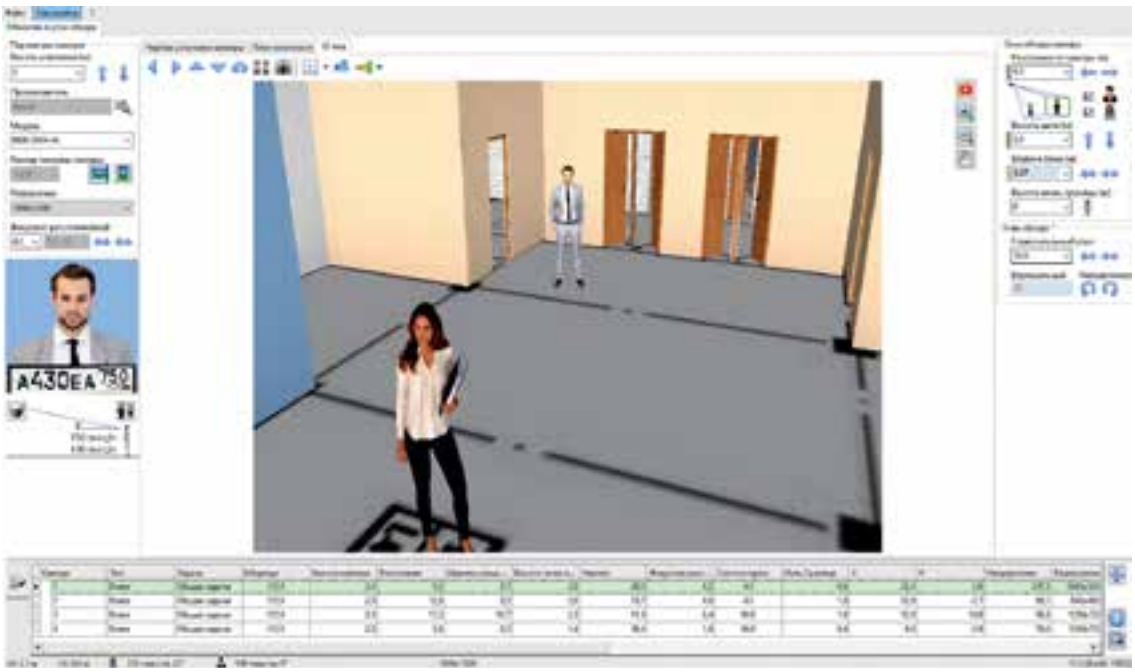


Рис. 4.
3D-вид с модели видеокамеры

Рис. 5.
Моделирование изображения с видеокамеры с цветовым обозначением зон: красный – идентификация, желтый – распознавание, зеленый – обнаружение

Рис. 6.
Реальное изображение с видеокамеры с разрешением 1920x1080 с указанием плотности пикселей на 1 метр

ВЫВОДЫ:

1. ***Качество изображения, получаемого с видеокамеры, должно соответствовать определенным требованиям в зависимости от задачи, поставленной перед оператором для установленной зоны наблюдения.***
2. ***Один из главных показателей, от которого зависит возможность решения поставленной перед оператором задачи, – плотность пикселей видеоизображения. Значение плотности пикселей зависит от разрешающей способности камеры, а также от расстояния от камеры до объекта интереса и угла обзора камеры.***
3. ***Качество изображения также зависит от факторов освещенности, места и угла установки видеокамеры, а также от траектории и скорости движения объектов в кадре.***
4. ***Для проверки соблюдения показателей плотности пикселей в той или иной области наблюдения рекомендуется использовать специализированное ПО для проектирования систем видеонаблюдения.***

ГЛАВА 5.3.
ОСНОВЫ ВЫБОРА КОЛИЧЕСТВА И МЕСТ РАЗМЕЩЕНИЯ ВИДЕОКАМЕР И ДРУГИХ ЭЛЕМЕНТОВ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

Выбор количества проектируемых (устанавливаемых) видеокамер должен быть обусловлен, прежде всего, теми задачами, которые возлагаются на внедряемую систему видеонаблюдения.

а) МОНИТОРИНГ. СБОР СТАТИСТИЧЕСКИХ ДАННЫХ. АНАЛИЗ ПРОИСШЕСТВИЙ

Для указанных функций систем видеонаблюдения в помещениях площадью более 25 квадратных метров целесообразно применять не менее двух видеокамер. В помещениях правильной прямоугольной формы камеры следует устанавливать на высоте 2,5–4 м в углах помещения диагонально или по одной из стен, в зависимости от сопутствующих условий. В условиях, когда планировочные решения оборудуемых помещений непостоянны (залы для временных выставок, трансформируемые пространства и т. п.) и высота потолков не превышает 4 метров, более эффективным может стать размещение мониторинговых видеокамер на конструкциях потолка. В таких случаях стоит рассмотреть применение видеокамер с изменяющимся фокусным расстоянием или широкоугольным объективом «рыбий глаз».

ВАЖНО! ***Если потолочное размещение оборудования не представляется возможным, следует предусмотреть дублирующие (размещенные на одной физической кабельной линии) или дополнительные точки подключения (сетевые розетки, закладные конструкции) на стенах и перегородках в местах возможного крепления видеокамер в случае перепланировки пространства.***

б) АВТОМАТИЗИРОВАННОЕ ОХРАННОЕ ТЕЛЕВИДЕНИЕ. ФУНКЦИИ ИДЕНТИФИКАЦИИ ОБЪЕКТОВ. ТЕРМОМЕТРИЯ

Для обеспечения эффективной работы системы видеонаблюдения с функциями автоматического анализа данных входящего видеопотока необходимо внимательно отнестись к выбору типов и размещению видеокамер.

Камеры для работы алгоритмов распознавания лиц и термометрии должны размещаться на высоте 1,8–2,3 м (условно допускается установка на уровне до 2,5 м). При выборе мест размещения следует отдать предпочтение входным зонам здания, пунктам досмотра, коридорам, дверным порталам, эскалаторам, лестничным маршам и иным местам, где объекту возможного поиска будет сложнее быстро перемещаться и скрываться от попадания в объектив.

Для детектирования оставленных/исчезнувших предметов следует по возможности использовать мониторинговые камеры, выделяя для аналитики об-

Таблица № 4

Основные требования к характеристикам, функциям и местам размещения видеокамер (скачать таблицу отдельным pdf-файлом >)

Место	Требования к позиционированию и просмотру зоны/места, задаче наблюдения и плотности пикселей	Требования к характеристикам камер	
1. **Въезд/выезд на территорию. Площадка досмотра автотранспорта**	**Въезд/выезд на территорию**: необходимо обеспечить просмотр всей зоны въезда для пресечения въезда другого транспорта вслед допущенного. Обеспечить просмотр всего створа ворот для выявления несанкционированного прохода людей при пропуске транспорта. Расположение камеры должно минимизировать влияние встречной засветки от света фар автомобиля. Целесообразно обеспечить двухсторонний обзор для контроля и идентификации как въезжающего, так и выезжающего транспорта, а также входящих и выходящих людей. **Площадка досмотра автотранспорта:** необходимо обеспечить просмотр всей зоны досмотра. Расположение камер подразумевает необходимость наблюдать как за процессом досмотра, так и за просмотром открытого кузова/багажника автомобиля. **Задача наблюдения:** идентификация людей и автотранспорта. **Плотность пикселей:** не менее 500 пикселей/метр.	**Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). Желательно использовать технологии, повышающие чувствительность в цветном режиме для фиксирования цвета автомобиля в условиях плохого освещения (цветная видеосъемка в ночное время от 0,012 лк). **Компенсация внешней засветки.** **Динамический диапазон:** не ниже 140 дБ. **Объектив[2]:** моторизованный вариофокальный объектив. Угол обзора подбирается в зависимости от расположения камер и конфигурации требуемой зоны наблюдения. **Вандалозащищенность:** класс защиты IK10 по стандарту IEC 62262. **Пылевлагозащищенность:** не хуже IP66 по стандарту IEC 60529. **Рабочая температура:** должна соответствовать условиям окружающей среды. **Дополнительные функции:** автоматическая настройка камеры под изменение сцены или освещение.	

На этой странице текст зеленого цвета содержит гиперссылку

ласти изображения, охватывающие тупиковые зоны помещений, гардеробы, зоны отдыха, стойки информации, музейные магазины и пр.

ВАЖНО! ***Для корректной работы такого алгоритма и минимизации ложных срабатываний в большинстве случаев необходимо, чтобы в зоне детектирования не было легко перемещаемых предметов (стулья, легкие скамейки, легкие мусорные корзины, мобильные плакаты и т. п.).***

Для обнаружения событий пересечения линии или входа в определенную область изображения также возможно использование мониторинговых камер видеонаблюдения. При выборе мест установки видеокамер следует учитывать вероятность негативного влияния перспективных размерных искажений, когда пересекаемая линия или контролируемая область расположены (вытянуты) вдоль оптической оси камеры. В таком случае сложнее задать диапазон допустимых размеров объекта, формирующего сигнал тревоги, и возрастает риск ложных срабатываний системы.

Если требуется организовать наружное видеонаблюдение, камеры в общем случае целесообразно устанавливать по периметру территории, в местах входа и выхода людей, вдоль прогулочных дорожек или иных путей их возможного перемещения, а также парковых сооружений. Следует размещать камеры на устойчивых строительных конструкциях. При выборе мест установки камер на фасадах зданий необходимо учитывать архитектурные особенности их конструкции. Обзору не должны препятствовать части водосточных систем, архитектурные элементы и т. п. Высота и места установки камер должны выбираться с учетом их регламентного обслуживания и ремонта без привлечения специализированной подъемной техники. Не следует размещать видеокамеры с длиннофокусными объективами на отдельно стоящих столбах или вышках из-за возможного негативного влияния колебаний последних под действием ветра и расфокусировки изображения.

Во всех случаях стоит обеспечить размещение каждой камеры в области охвата как минимум еще одной.

ВАЖНО! ***Следует избегать размещения видео камер напротив возможного источника прямого света или рядом с таким источником и не следует ориентировать видеокамеру в сторону близко расположенных объектов или допускать нахождения в кадре большой части конструкции, на которой она установлена, из-за возможного чрезмерного отраженного излучения от источника ИК-подсветки видеокамеры в ночном режиме.***

В таблице № 4 приведены краткие рекомендации по организации размещения видеокамер для некоторых наиболее часто выделяемых зон **(скачать таблицу отдельным pdf-файлом >**).

	Требования к качеству изображения[1]	Функции	
	a) освещенность в зоне регистрации – от 100 ±10 до 1000 ±50 люкс (для камер без ИК-подсветки); b) дистанция съемки – от 1 до 40 м; c) данные изображения номера ГРЗ с угловыми координатами наклона и отклонения пластины – в диапазоне от 0 до 30 ±2 градусов; d) размер номера по горизонтали на изображении – не менее 120 Пикс; e) разрешение видеокамеры – от 1,3 Пикс; f) частота кадров – не менее 12 кадров в секунду; g) цветность регистрируемого видеоизображения – цветное или черно-белое; h) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 42 дБ.	**Рекомендуемое разрешение камеры[3]**	не менее 1,3 МПикс
		Звук	нет
		Тепловизионная съемка	нет
		ИК-подсветка (встроенная/внешняя)	да
		Возможная аналитика	распознавание госномеров автотранспорта; детектор движения; подсчет транспорта/людей; классификация транспорта; проход людей в запрещенную зону; идентификация людей; проход или проезд в запрещенном направлении.

На этой странице текст зеленого цвета содержит гиперссылку

На этой странице текст зеленого цвета содержит гиперссылку

Таблица № 4 Продолжение (скачать таблицу отдельным pdf-файлом >)

Место	Требования к позиционированию и просмотру зоны/места, задаче наблюдения и плотности пикселей	Требования к характеристикам камер	
2. Вызывное устройство (видеодомофон)	Определяется исходя из требований к качеству изображений в части получаемого ракурса лица. **Задача наблюдения:** идентификация людей. **Плотность пикселей:** не менее 250 пикселей/метр.	**Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Компенсация внешней засветки.** **Динамический диапазон:** не ниже 140 дБ. **Объектив:** моторизованный объектив. Угол обзора подбирается в зависимости от расположения камер. **Вандалозащищенность:** класс защиты IK10 по стандарту IEC 62262. **Пылевлагозащищенность:** не хуже IP66 по стандарту IEC 60529. **Рабочая температура:** должна соответствовать условиям окружающей среды. **Дополнительные функции:** автоматическая настройка камеры под изменение сцены или освещение.	
3. Входы (выходы) в здание, в том числе эвакуационные, калитки, двери во внешнем ограждении	Возможность идентификации человека, распознавание лиц. **Задача наблюдения:** идентификация людей. **Плотность пикселей:** не менее 500 пикселей/метр.	**Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Компенсация внешней засветки.** **Динамический диапазон:** не ниже 140 дБ. **Объектив:** моторизованный объектив. Угол обзора подбирается в зависимости от расположения камер. **Вандалозащищенность:** класс защиты IK10 по стандарту IEC 62262. **Пылевлагозащищенность:** не хуже IP66 по стандарту IEC 60529. **Рабочая температура:** должна соответствовать условиям окружающей среды. **Дополнительные функции:** автоматическая настройка камеры под изменение сцены или освещение.	
4. Внешний периметр территории	Попадание в кадр как конструкции объектов, так и прилегающей территории. Качество изображения должно быть достаточным для возможности обнаружить и распознать действия нарушителя. **Задача наблюдения:** обнаружение людей. **Плотность пикселей:** не менее 25 пикселей/метр, желательно 62 пикселя/м.	**Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Динамический диапазон:** не ниже 120 дБ. **Объектив:** моторизованный, с углом обзора 45–90°. **Вандалозащищенность:** класс защиты IK10 по стандарту IEC 62262. **Пылевлагозащищенность:** не хуже IP66 по стандарту IEC 60529. **Рабочая температура:** должна соответствовать условиям окружающей среды. **Дополнительные функции:** автоматическая настройка камеры под изменение сцены или освещение; для узких протяженных зон целесообразно использовать коридорный формат.	

	Требования к качеству изображения[1]	Функции	
	a) освещенность в плоскости лица – от 100 ±10 до 1000 ±50 люкс; b) неравномерность освещенности лица – не более (50 ±5) процентов; c) разрешение видеоизображения, обеспечивающее регистрацию изображений лиц на рабочей дистанции съемки видеокамеры не менее 1,5 м с расстоянием между центрами глаз не менее 60 пикселей; d) динамический диапазон интенсивности изображения в области лица – не менее 8 бит; цветность видеоизображения – черно-белое; частота – не менее 16 кадров в секунду; e) ракурс лица относительно фронтального ракурса, определяемый в соответствии с ГОСТ Р ИСО/МЭК 19794-5-2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица» угловыми координатами поворота, наклона и отклонения лица: в диапазоне от 0 до 15 ±2 градусов; f) структура фона (подвижный случайно неоднородный фон съемки с перепадами контраста) – от 0,2 ±0,05 до 0,8 ±0,05; g) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 45 дБ; h) дисторсия – не более 5 процентов (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).	**Ориентировочное разрешение камеры**	не менее 1,3 Мпикс
		Звук	да
		Тепловизионная съемка	возможно, для вызовных устройств внутреннего исполнения
		ИК-подсветка (встроенная, внешняя)	нет
		Возможная аналитика	распознавание лиц; определение температуры тела человека; наличие маски на лице.
	a) освещенность в плоскости лица – от (100 ±10) до (1000 ±50) люкс; b) неравномерность освещенности лица – не более (50 ±5) процентов; c) разрешение видеоизображения, обеспечивающее регистрацию изображений лиц на рабочей дистанции съемки видеокамеры не менее 1,5 метра с расстоянием между центрами глаз не менее 60 пикселей; d) динамический диапазон интенсивности изображения в области лица – не менее 8 бит; цветность видеоизображения – черно-белое; частота – не менее 16 кадров в секунду; e) ракурс лица относительно фронтального ракурса, определяемый в соответствии с ГОСТ Р ИСО/МЭК 19794-5-2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица» угловыми координатами поворота, наклона и отклонения лица: в диапазоне от 0 до 15 ±2 градусов; f) структура фона (подвижный случайно неоднородный фон съемки с перепадами контраста) – от 0,2 ±0,05 до 0,8 ±0,05; g) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 45 дБ; h) дисторсия – не более 5 процентов (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).	**Ориентировочное разрешение камеры**	Full HD (1920x1080)
		Звук	нет
		Тепловизионная съемка	нет
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	распознавание лиц; реидентификация; проход людей в запрещенную зону; проход в запрещенном направлении.
	a) освещенность в зоне регистрации – от 100 ±10 до 1000 ±50 люкс (для камер без ИК-подсветки); b) дистанция съемки – от 5 до 30 метров; c) угол наклона оптической оси видеокамеры относительно горизонтальной плоскости – не менее 15 градусов (для наклонного способа размещения), 90 ±10 градусов (для потолочного способа размещения); d) разрешение видеокамеры – от 2 МПикс; e) плотность потока людей – не более 1 чел./м^2; f) объем оставленного предмета – от 3 дм^3; g) структура фона – подвижный случайно неоднородный фон съемки с перепадами контраста от 0,2 ±0,05 до 0,8 ±0,05; h) частота кадров – не менее 25 кадров в секунду; i) цветность регистрируемого видеоизображения – цветное; j) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 42 дБ; k) дисторсия – не более 10 процентов (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).	**Ориентировочное разрешение камеры**	Full HD (1920x1080)
		Звук	нет
		Тепловизионная съемка	нет
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	проход людей в запрещенную зону; оставленные/отсутствующие предметы; классификация объектов в кадре.

На этой странице текст зеленого цвета содержит гиперссылку

Таблица № 4 Продолжение (скачать таблицу отдельным pdf-файлом >)

Место	Требования к позиционированию и просмотру зоны/места, задаче наблюдения и плотности пикселей	Требования к характеристикам камер	
5. Территория, прилегающая к зданию, относящемуся к объекту культурного наследия или использующемуся для демонстрации (хранения) произведений и предметов культуры, включая стоянки для автотранспорта	Обзорное видеонаблюдение для фиксирования нештатных ситуаций без подробной детализации в сочетании с PTZ-камерой(-ами) для возможности получить подробную видеоинформацию. **Задача наблюдения:** наблюдение. **Плотность пикселей:** не менее 62 пикселей/метр для фиксированных камер, не менее 250 пикселей/метр для PTZ-камер.	**ФИКСИРОВАННЫЕ КАМЕРЫ** **Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Динамический диапазон:** не ниже 120 дБ. **Объектив:** фиксированный объектив с углом обзора около 100° для покрытия большей территории меньшим количеством камер. **Вандалозащищенность:** класс защиты IK10 по стандарту IEC 62262. **Пылевлагозащищенность:** не хуже IP66 по стандарту IEC 60529. **Рабочая температура:** должна соответствовать условиям окружающей среды. **Дополнительные функции:** автоматическая настройка камеры под изменение сцены или освещение. **PTZ-КАМЕРЫ** **Разрешение:** не ниже Full HD. **Объектив:** объектив с углом обзора 3,4–73° или лучше. Это соответствует 21x увеличению. Окончательный выбор угла обзора зависит от расположения камеры и площади, которую она должна покрывать. **Дополнительные функции:** Автослежение за объектом (автоматическое или по сигналу со стационарной камеры). Покрытие купола ClearSight (для снижения загрязнения и уменьшения стоимости техобслуживания и улучшения видеоизображения).	
6. Входная дверь	Направление камер на двери, то есть области с сильной встречной засветкой. Расположение камеры должно минимизировать влияние встречной засветки. **Задача наблюдения:** идентификация. **Плотность пикселей:** не менее 250 пикселей/метр.	**Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Компенсация внешней засветки.** **Динамический диапазон:** не ниже 140 дБ. **Объектив:** моторизованный объектив с углом обзора 30–70° или с бóльшим диапазоном. Угол обзора подбирается в зависимости от расположения камер. Также данный тип камер может быть использован совместно с системами распознавания лиц. **Дополнительные функции** автоматическая настройка камеры под изменение сцены или освещение.	
7. Место досмотра	Видеокамеры должны обеспечивать возможность идентификации человека и фиксировать процедуру досмотра для исключения спорных ситуаций. **Задача наблюдения:** идентификация. **Плотность пикселей:** не менее 250 пикселей/метр.	**Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Компенсация внешней засветки.** **Динамический диапазон:** не ниже 140 дБ. **Объектив:** моторизованный объектив с углом обзора 30–70° или с бóльшим диапазоном. Угол обзора подбирается в зависимости от расположения камер.	

	Требования к качеству изображения[1]	Функции	
	a) освещенность в зоне регистрации – от 100 ±10 до 1000 ±50 люкс (для камер без ИК-подсветки); b) дистанция съемки – от 5 до 30 метров; c) угол наклона оптической оси видеокамеры относительно горизонтальной плоскости – не менее 15 градусов (для наклонного способа размещения), 90 ±10 градусов (для потолочного способа размещения); d) разрешение видеокамеры – от 2 Мпикс; e) плотность потока людей – не более 1 чел./м^2; f) объем оставленного предмета – от 3 дм^3; g) структура фона – подвижный случайно неоднородный фон съемки с перепадами контраста от 0,2 ±0,05 до 0,8 ±0,05; h) частота кадров – не менее 25 кадров в секунду; i) цветность регистрируемого видеоизображения – цветное; j) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 42 дБ; k) дисторсия – не более 10 процентов (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).	**Ориентировочное разрешение камеры**	Full HD (1920x1080)
		Звук	нет
		Тепловизионная съемка	нет
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	проход в запрещенную зону; оставленные предметы; классификация объектов в кадре; обнаружение аномалий в сцене; обнаружение праздношатания.
	a) освещенность в плоскости лица – от 100 ±10 до 1000 ±50 люкс; b) неравномерность освещенности лица – не более 50 ±5 процентов; c) разрешение видеоизображения, обеспечивающее регистрацию изображений лиц на рабочей дистанции съемки видеокамеры не менее 1,5 м с расстоянием между центрами глаз не менее 60 пикселей; d) динамический диапазон интенсивности изображения в области лица – не менее 8 бит; цветность видеоизображения – черно-белое; частота – не менее 16 кадров в секунду; e) ракурс лица относительно фронтального ракурса, определяемый в соответствии с ГОСТ Р ИСО/МЭК 19794-5-2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица» угловыми координатами поворота, наклона и отклонения лица – в диапазоне от 0 до 15 ±2 градусов; f) структура фона (подвижный случайно неоднородный фон съемки с перепадами контраста) – от 0,2 ±0,05 до 0,8 ±0,05; g) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 45 дБ; h) дисторсия – не более 5 процентов (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).	**Ориентировочное разрешение камеры**	Full HD (1920x1080)
		Звук	нет
		Тепловизионная съемка	возможно для камер внутреннего исполнения
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	проход людей в запрещенную зону; оставленные/отсутствующие предметы; классификация объектов в кадре; идентификация людей.
	аналогично п. 2 в части распознавания лиц и п. 4 для прочей видеоаналитики	**Ориентировочное разрешение камеры**	Full HD (1920x1080)
		Звук	да
		Тепловизионная съемка	возможно
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	распознавание лиц; реидентификация; измерение температуры; ношение маски и иных СИЗ; контроль проведения досмотровых мероприятий.

На этой странице текст зеленого цвета содержит гиперссылку

Таблица № 4 Продолжение (скачать таблицу отдельным pdf-файлом >)

Место	Требования к позиционированию и просмотру зоны/места, задаче наблюдения и плотности пикселей	Требования к характеристикам камер	
8. Вестибюль, входная зона	Обзорное видеонаблюдение для фиксирования нештатных ситуаций без подробной детализации. **Задача наблюдения:** наблюдение. **Плотность пикселей:** не менее 62 пикселей/метр.	**Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Динамический диапазон:** не ниже 120 дБ. **Объектив:** фиксированный объектив с углом обзора около 100° для покрытия большей территории меньшим количеством камер. **Дополнительные функции** автоматическая настройка камеры под изменение сцены или освещение.	
9. Касса, гардероб, камера хранения, администратор, стойка информации	Видеокамеры должны обеспечивать возможность идентификации человека и проведенных операций кассиром/посетителем, включая зону передачи товарно-материальных ценностей. **Задача наблюдения:** распознавание для вспомогательных частей зоны и идентификация для зон проведения операций. **Плотность пикселей:** не менее 125 и 500 пикселей/метр соответственно.	**Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Компенсация внешней засветки.** **Динамический диапазон:** не ниже 120 дБ. **Объектив:** моторизованный объектив с углом обзора 45–100°.	
10. Магазин, кафе (кроме кассовых зон)	Обзорное видеонаблюдение для фиксирования нештатных ситуаций без подробной детализации. **Задача наблюдения:** наблюдение. **Плотность пикселей:** не менее 62 пикселей/метр.	**Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Динамический диапазон:** не ниже 120 дБ. **Объектив:** фиксированный объектив с углом обзора около 100 для покрытия большей территории меньшим количеством камер. **Дополнительные функции:** автоматическая настройка камеры под изменение сцены или освещение.	
11. Администрация	Обзорное видеонаблюдение для фиксирования нештатных ситуаций без подробной детализации. **Задача наблюдения:** наблюдение. **Плотность пикселей:** не менее 62 пикселей/метр.	**Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Динамический диапазон:** не ниже 120 дБ. **Объектив:** фиксированный объектив с углом обзора около 100° для покрытия большей территории меньшим количеством камер. **Дополнительные функции:** автоматическая настройка камеры под изменение сцены или освещение.	

	Требования к качеству изображения[1]	Функции	
	a) освещенность в зоне регистрации – от 100 ±10 до 1000 ±50 люкс (для камер без ИК-подсветки); b) дистанция съемки – от 5 до 30 метров; c) угол наклона оптической оси видеокамеры относительно горизонтальной плоскости: не менее 15 градусов (для наклонного способа размещения); 90 ±10 градусов (для потолочного способа размещения); d) разрешение видеокамеры – от 2 МПикс˘ ; e) плотность потока людей – не более 1 чел./м^2; f) объем оставленного предмета – от 3 дм^3; g) структура фона – подвижный случайно неоднородный фон съемки с перепадами контраста от 0,2 ±0,05 до 0,8 ±0,05; h) частота кадров – не менее 25 кадров в секунду; i) цветность регистрируемого видеоизображения – цветное; j) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 42 дБ; k) дисторсия – не более 10 процентов (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).	**Ориентировочное разрешение камеры**	Full HD (1920x1080)
		Звук	нет
		Тепловизионная съемка	нет
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	проход людей в запрещенную зону; оставленные/отсутствующие предметы; классификация объектов в кадре.
	аналогично п. 2 в части пола/возраста/эмоций и п. 4 для прочей видеоаналитики	**Ориентировочное разрешение камеры**	Full HD (1920x1080)
		Звук	да
		Тепловизионная съемка	нет
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	речевая аналитика; интеграция с POS-терминалом; определение пола/возраста/эмоций; подсчет посетителей.
	a) освещенность в зоне регистрации – от 100 ±10 до 1000 ±50 люкс (для камер без ИК-подсветки); b) дистанция съемки – от 5 до 30 метров; c) угол наклона оптической оси видеокамеры относительно горизонтальной плоскости – не менее 15 градусов (для наклонного способа размещения), 90 ±10 градусов (для потолочного способа размещения); d) разрешение видеокамеры – от 2 МПикс; e) плотность потока людей – не более 1 чел./м^2; f) объем оставленного предмета – от 3 дм^3; g) структура фона – подвижный случайно неоднородный фон съемки с перепадами контраста от 0,2 ±0,05 до 0,8 ±0,05; h) частота кадров – не менее 25 кадров в секунду; i) цветность регистрируемого видеоизображения – цветное; j) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 42 дБ; k) дисторсия – не более 10 процентов (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).	**Ориентировочное разрешение камеры**	Full HD (1920x1080)
		Звук	да
		Тепловизионная съемка	нет
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	проход людей в запрещенную зону; оставленные/отсутствующие предметы; классификация объектов в кадре.
	a) освещенность в зоне регистрации – от 100 ±10 до 1000 ±50 люкс (для камер без ИК-подсветки); b) дистанция съемки – от 5 до 30 метров; c) угол наклона оптической оси видеокамеры относительно горизонтальной плоскости – не менее 15 градусов (для наклонного способа размещения), 90 ±10 градусов (для потолочного способа размещения); d) разрешение видеокамеры – от 2 мегапикселей; e) плотность потока людей – не более 1 чел./м^2; f) объем оставленного предмета – от 3 дм^3; g) структура фона – подвижный случайно неоднородный фон съемки с перепадами контраста от 0,2 ±0,05 до 0,8 ±0,05; h) частота кадров – не менее 25 кадров в секунду; i) цветность регистрируемого видеоизображения – цветное; j) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 42 дБ; k) дисторсия – не более 10 процентов (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).	**Ориентировочное разрешение камеры**	Full HD (1920x1080)
		Звук	нет
		Тепловизионная съемка	нет
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	проход людей в запрещенную зону; оставленные/отсутствующие предметы; классификация объектов в кадре.

На этой странице текст зеленого цвета содержит гиперссылку

Таблица № 4 Продолжение (скачать таблицу отдельным pdf-файлом >)

Место	Требования к позиционированию и просмотру зоны/места, задаче наблюдения и плотности пикселей	Требования к характеристикам камер	
12. Экспозиционные залы	Обзорное видеонаблюдение без «мертвых зон» для фиксирования нештатных ситуаций без подробной детализации в сочетании с видеонаблюдением за входами/выходами. **Задача наблюдения:** наблюдение для залов и распознавание для входов/выходов. **Плотность пикселей:** не менее 62 и 125 пикселей/метр соответственно.	**ОБЗОРНЫЕ КАМЕРЫ** **Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Динамический диапазон:** не ниже 120 дБ. **Объектив:** фиксированный объектив с углом обзора около 100° для покрытия большей территории меньшим количеством камер. **ВИДЕОКАМЕРЫ НА ВХОДАХ/ВЫХОДАХ** **Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Динамический диапазон:** не ниже 120 дБ. **Объектив:** моторизованный объектив с углом обзора 45–100°.	
13. Помещения хранения и реставрационных лабораторий, склады, критически важные технические помещения, лифты, подходы к фондохранилищам	Обзорное видеонаблюдение без «мертвых зон» для фиксирования нештатных ситуаций без подробной детализации в сочетании с видеонаблюдением за входами/выходами. Обзорное видеонаблюдение за действием персонала (идентификация/распознавание + интеграция СКУД). **Задача наблюдения:** наблюдение для лабораторий, складов, критически важных технических помещений и распознавание для лифтов и подходов. **Плотность пикселей:** не менее 62 и 125 пикселей/метр соответственно.	**Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Динамический диапазон:** не ниже 120 дБ. **Объектив:** фиксированный объектив с углом обзора около 100° для покрытия большей территории меньшим количеством камер. **Дополнительные функции:** автоматическая настройка камеры под изменение сцены или освещение.	
14. Помещения временных выставок (залы с частой сменой экспозиции)	Наличие комплекта оборудования для быстрой организации локального видеонаблюдения с выводом на центральный пульт (либо наличие бюджета для заключения договора на предоставление такого оборудования и выполнения работ). **Задача наблюдения:** наблюдение для залов в соответствии с конфигурацией экспозиции и распознавание для входов/выходов. **Плотность пикселей:** не менее 62 и 125 пикселей/метр соответственно.	**ОБЗОРНЫЕ КАМЕРЫ** **Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Динамический диапазон:** не ниже 120 дБ. **Объектив:** фиксированный объектив с углом обзора около 100° для покрытия большей территории меньшим количеством камер. **ВИДЕОКАМЕРЫ НА ВХОДАХ/ВЫХОДАХ** **Чувствительность:** цветной режим: 0,01 лк, черно-белый режим: 0 лк (ИК). **Динамический диапазон:** не ниже 120 дБ. **Объектив:** моторизованный объектив с углом обзора 45–100°.	

	Требования к качеству изображения[1]	Функции	
	a) освещенность в зоне регистрации – от 100 ±10 до 1000 ±50 люкс (для камер без ИК-подсветки); b) дистанция съемки – от 5 до 30 метров; c) угол наклона оптической оси видеокамеры относительно горизонтальной плоскости – не менее 15 градусов (для наклонного способа размещения), 90 ±10 градусов (для потолочного способа размещения); d) разрешение видеокамеры – от 2 МПикс; e) плотность потока людей – не более 1 чел./м^2; f) объем оставленного предмета – от 3 дм^3; g) структура фона – подвижный случайно неоднородный фон съемки с перепадами контраста от 0,2 ±0,05 до 0,8 ±0,05; h) частота кадров – не менее 25 кадров в секунду; i) цветность регистрируемого видеоизображения – цветное; j) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 42 дБ; k) дисторсия – не более 10 процентов (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).	**Ориентировочное разрешение камеры**	не менее Full HD (1920x1080), для бóльших площадей возможно использование камер с разрешением 8 МПикс и выше
		Звук	нет
		Тепловизионная съемка	нет
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	проход людей в запрещенную зону; оставленные/отсутствующие предметы; классификация объектов в кадре; тепловые карты; зоны внимания.
	a) освещенность в зоне регистрации – от 100 ±10 до 1000 ±50 люкс (для камер без ИК-подсветки); b) дистанция съемки – от 5 до 30 метров; c) угол наклона оптической оси видеокамеры относительно горизонтальной плоскости – не менее 15 градусов (для наклонного способа размещения), 90 ±10 градусов (для потолочного способа размещения); d) разрешение видеокамеры – от 2 МПикс; e) плотность потока людей – не более 1 чел./м^2; f) объем оставленного предмета – от 3 дм^3; g) структура фона – подвижный случайно неоднородный фон съемки с перепадами контраста от 0,2 ±0,05 до 0,8 ±0,05; h) частота кадров – не менее 25 кадров в секунду; i) цветность регистрируемого видеоизображения – цветное; j) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 42 дБ; k) дисторсия – не более 10 процентов (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).	**Ориентировочное разрешение камеры**	Full HD (1920x1080)
		Звук	нет
		Тепловизионная съемка	нет
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	проход людей в запрещенную зону; оставленные/отсутствующие предметы; классификация объектов в кадре; контроль производственных процессов.
	a) освещенность в зоне регистрации – от 100 ±10 до 1000 ±50 люкс (для камер без ИК-подсветки); b) дистанция съемки – от 5 до 30 метров; c) угол наклона оптической оси видеокамеры относительно горизонтальной плоскости – не менее 15 градусов (для наклонного способа размещения), 90 ±10 градусов (для потолочного способа размещения); d) разрешение видеокамеры – от 2 МПикс; e) плотность потока людей – не более 1 чел./м^2; f) объем оставленного предмета – от 3 дм^3; g) структура фона – подвижный случайно неоднородный фон съемки с перепадами контраста от 0,2 ±0,05 до 0,8 ±0,05; h) частота кадров – не менее 25 кадров в секунду; i) цветность регистрируемого видеоизображения – цветное; j) максимальное отношение сигнал/шум (с выключенной функцией автоматического усиления сигнала) – не менее 42 дБ; k) дисторсия – не более 10 процентов (по краям кадра – на расстоянии одной третьей ширины, высоты и диагоналей кадра от его центра).	**Ориентировочное разрешение камеры**	не менее Full HD (1920x1080), для больших площадей возможно использование камер с разрешением 8 МПикс и выше
		Звук	нет
		Тепловизионная съемка	нет
		ИК-подсветка (встроенная, внешняя)	да
		Возможная аналитика	проход людей в запрещенную зону; оставленные/отсутствующие предметы; классификация объектов в кадре; тепловые карты; зоны внимания.

ГЛАВА
5.4.
ТИПОВЫЕ РЕШЕНИЯ ПО РЕАЛИЗАЦИИ ВИДЕОНАБЛЮДЕНИЯ ДЛЯ РАЗЛИЧНЫХ КАТЕГОРИЙ ОБЪЕКТОВ

В предыдущей главе описаны основные рекомендации по расположению видеокамер с указанием основных требований к получаемому изображению. В качестве наглядного примера описанных рекомендаций предлагается воспользоваться моделью, схематично отражающей основные помещения и объекты, встречающиеся на территории музейных комплексов. Основная задача данного раздела – на примере показать принципы расположения видеокамер для обеспечения задач безопасности.

Рис. 7.
Расшифровка зон плотности пикселей на схемах

5.4.1.
ПЕРИМЕТР ОБЪЕКТА

Задачи – наблюдение и распознавание. Дальность съемки для каждой камеры не превышает 30 м. Весь периметр охвачен видеонаблюдением, без слепых зон.

Рис. 8. Периметральное видеонаблюдение

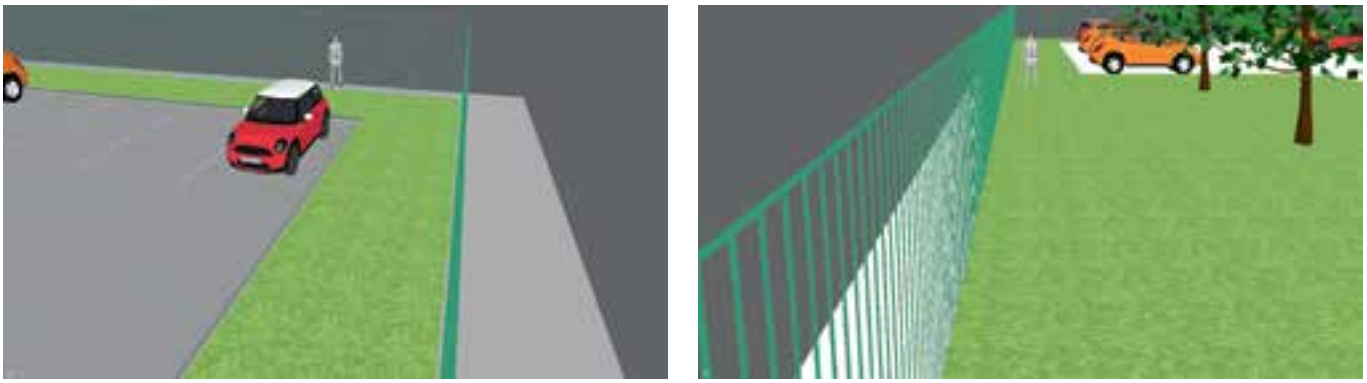


Рис. 8.1. Периметральное видеонаблюдение. Предполагаемое изображение с видеокамер

5.4.2.
ЗОНА ВХОДА НА ТЕРРИТОРИЮ, ВЪЕЗДНЫЕ ВОРОТА, ДОСМОТР АВТОМОБИЛЕЙ

Предполагаются отдельные стационарные видеокамеры для идентификации входящих на территорию посетителей, регистрации номерных знаков. Обзорное наблюдение зоны досмотра автомобилей, а также в КПП.

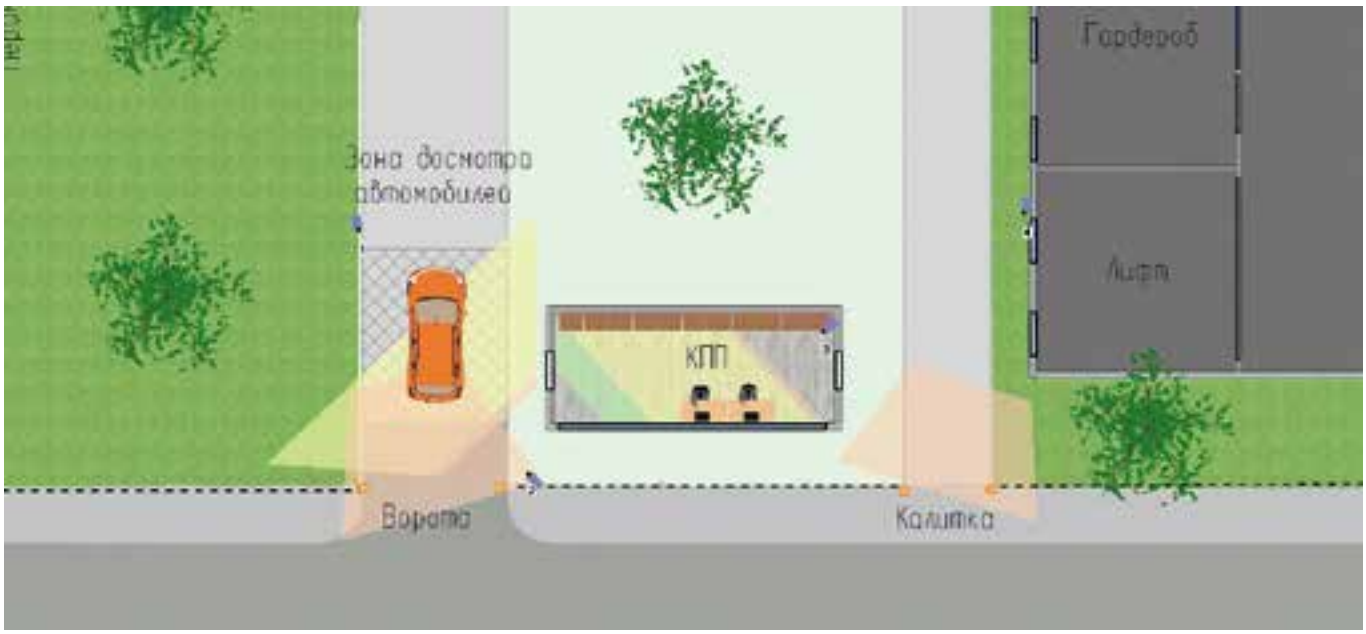


Рис. 9. Вход на территорию

Рис. 9.1. Вход на территорию. Предполагаемое изображение с видеокамер

5.4.3.
ВНУТРЕННЯЯ ТЕРРИТОРИЯ, ПАРКОВКА И ЗОНА РАЗМЕЩЕНИЯ УЛИЧНОГО ЭКСПОНАТА

Зона оснащается несколькими стационарными видеокамерами для обзорного наблюдения, рекомендуется установка PTZ-видеокамеры для детализации событий.

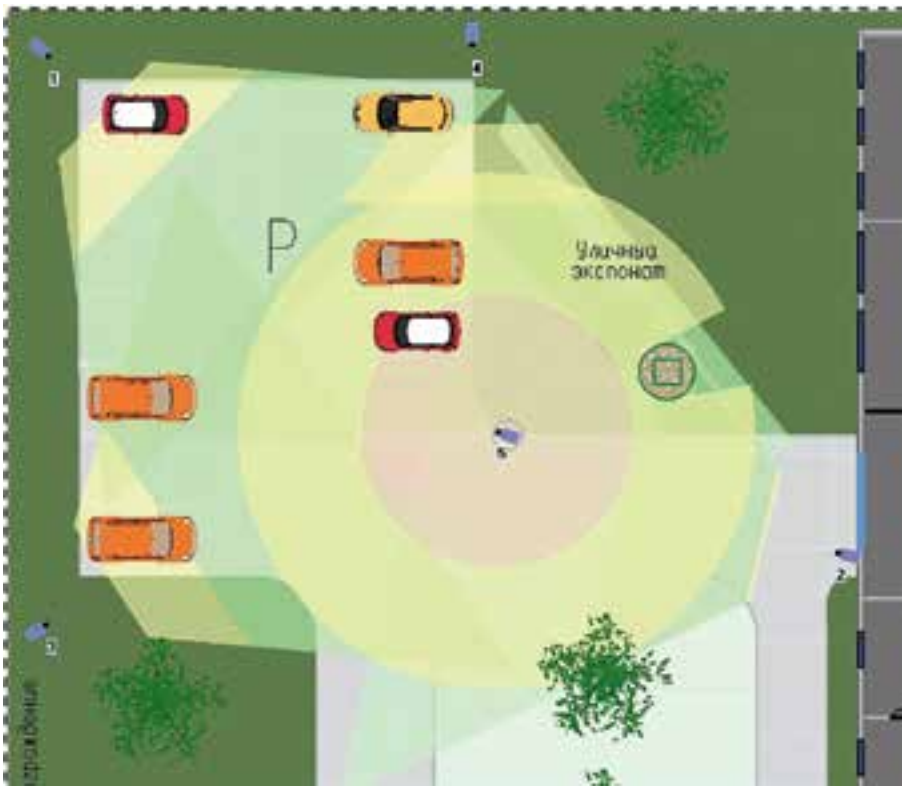


Рис. 10.
Внутренняя территория, паркинг

Рис. 10.1. Внутренняя территория, паркинг. Предполагаемое изображение с видеокамер

5.4.4.
ВХОДНАЯ ЗОНА

Входная зона оснащена двумя широкоугольными видеокамерами для оценки общей ситуации без слепых зон, направленной видеокамерой для идентификации лиц, входящих в здание.

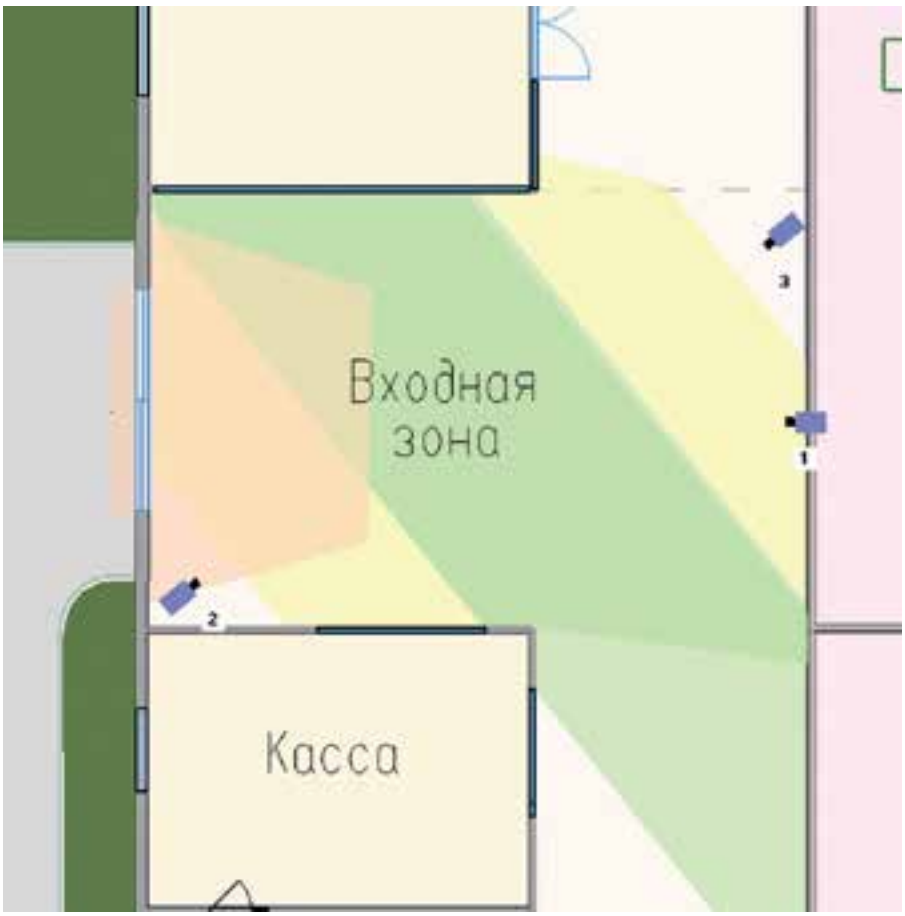


Рис. 11.
Входная зона

Рис. 11.1. Входная зона. Предполагаемое изображение с видеокамер

5.4.4.
КАССА

Помещение кассы оснащено тремя видеокамерами, фиксирующими все действия кассира и посетителей.

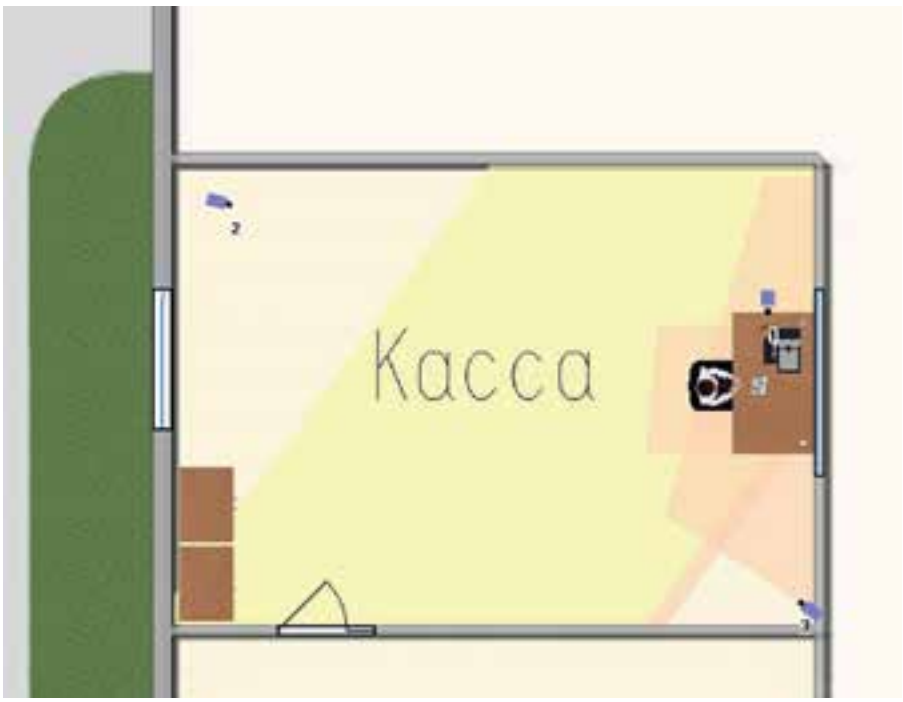


Рис. 12.
Касса

Рис. 12.1. Касса. Предполагаемое изображение с видеокамер

5.4.5.
ЗОНА КОНТРОЛЯ БИЛЕТОВ

В зоне контроля билетов предполагается идентификация входящих на экспозицию людей и отслеживание их действий.

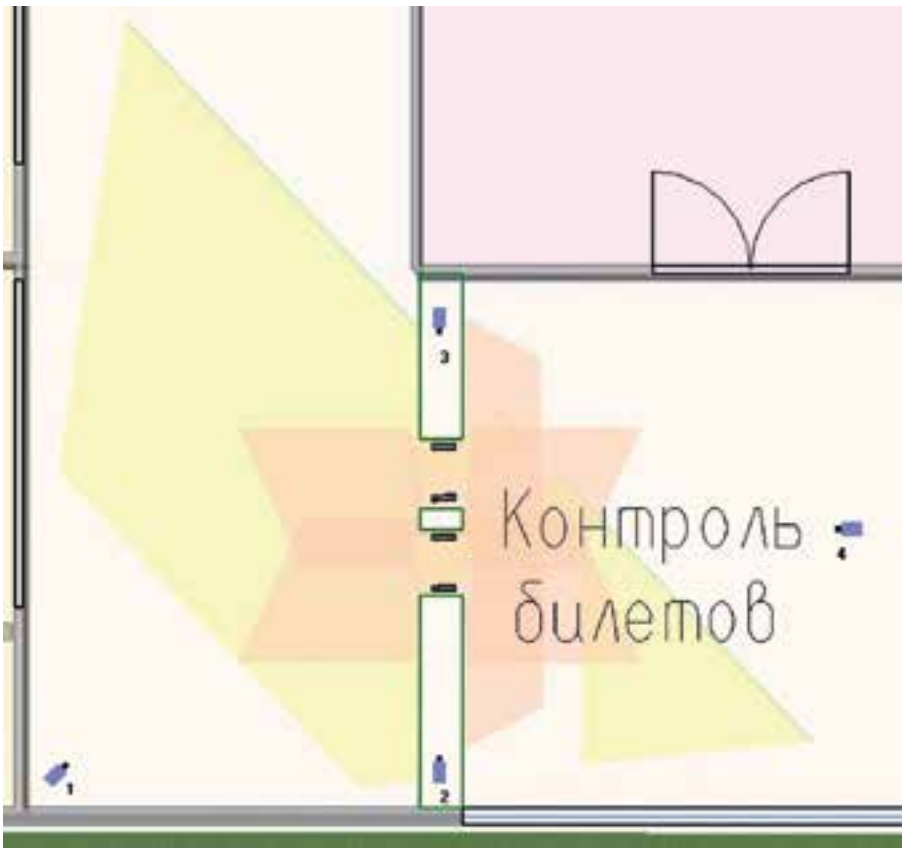


Рис. 13.
Контроль билетов

Рис. 13.1. Контроль билетов. Предполагаемое изображение с видеокамер

5.4.6.
КАРТИННАЯ ГАЛЕРЕЯ

Зал с наличием экспонатов оснащается видеокамерами, обеспечивающими наблюдение по всей площади без слепых зон. В центре зала расположена панорамная видеокамера с fisheye-объективом – она обеспечивает круговой обзор всех стен с экспонатами.

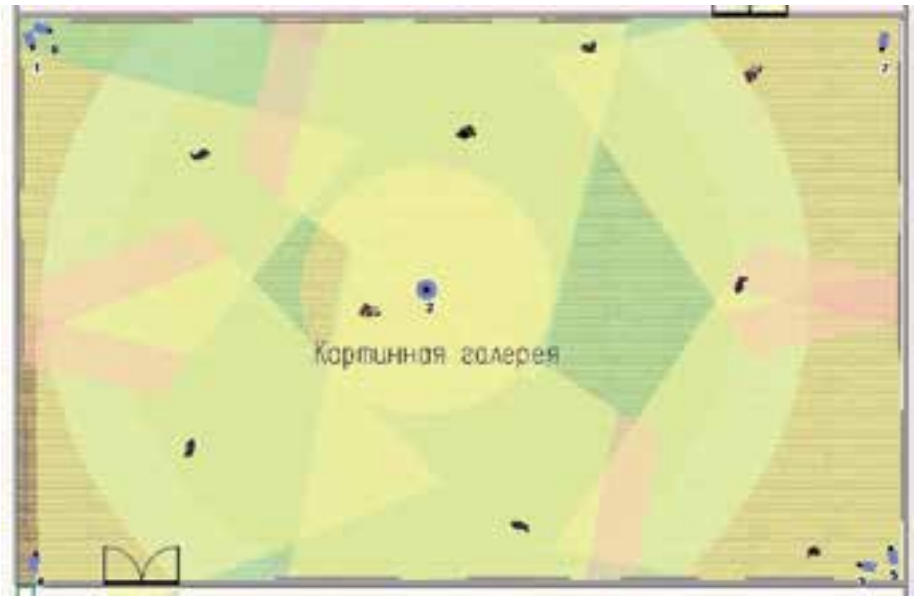


Рис. 14.
Картинная галерея

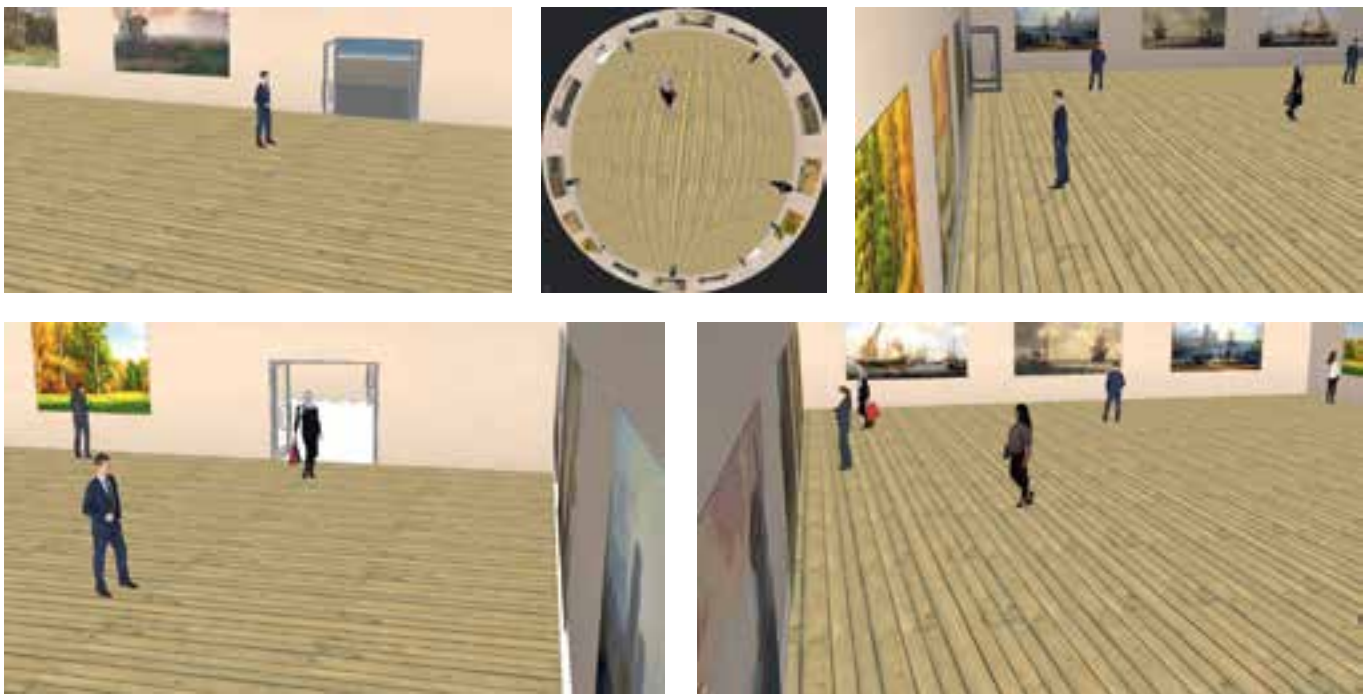


Рис. 14.1. Картинная галерея. Предполагаемое изображение с видеокамер

5.4.7.
ЗАЛ ВРЕМЕННОЙ ВЫСТАВКИ (С ЧАСТО СМЕНЯЕМОЙ ЭКСПОЗИЦИЕЙ)

Видеокамеры размещаются по всему периметру зала, охватывая все области с учетом перекрытий от экспонатов. При смене экспозиции возможна быстрая настройка видеокамер в новых положениях.

Рис. 15. Зал временных выставок

Рис. 15.1. Зал временных выставок.
Предполагаемое изображение с видеокамер

5.4.8.
ПОМЕЩЕНИЯ ПОВЫШЕННОЙ ВАЖНОСТИ – ХРАНИЛИЩЕ, РЕСТАВРАЦИОННАЯ ЛАБОРАТОРИЯ, ТЕХНИЧЕСКОЕ ПОМЕЩЕНИЕ

А) Б) В)

Рис. 16. Служебные помещения особой важности (А – общий план, Б – вход в коридор, техническое помещение, В – хранилище и лаборатория)

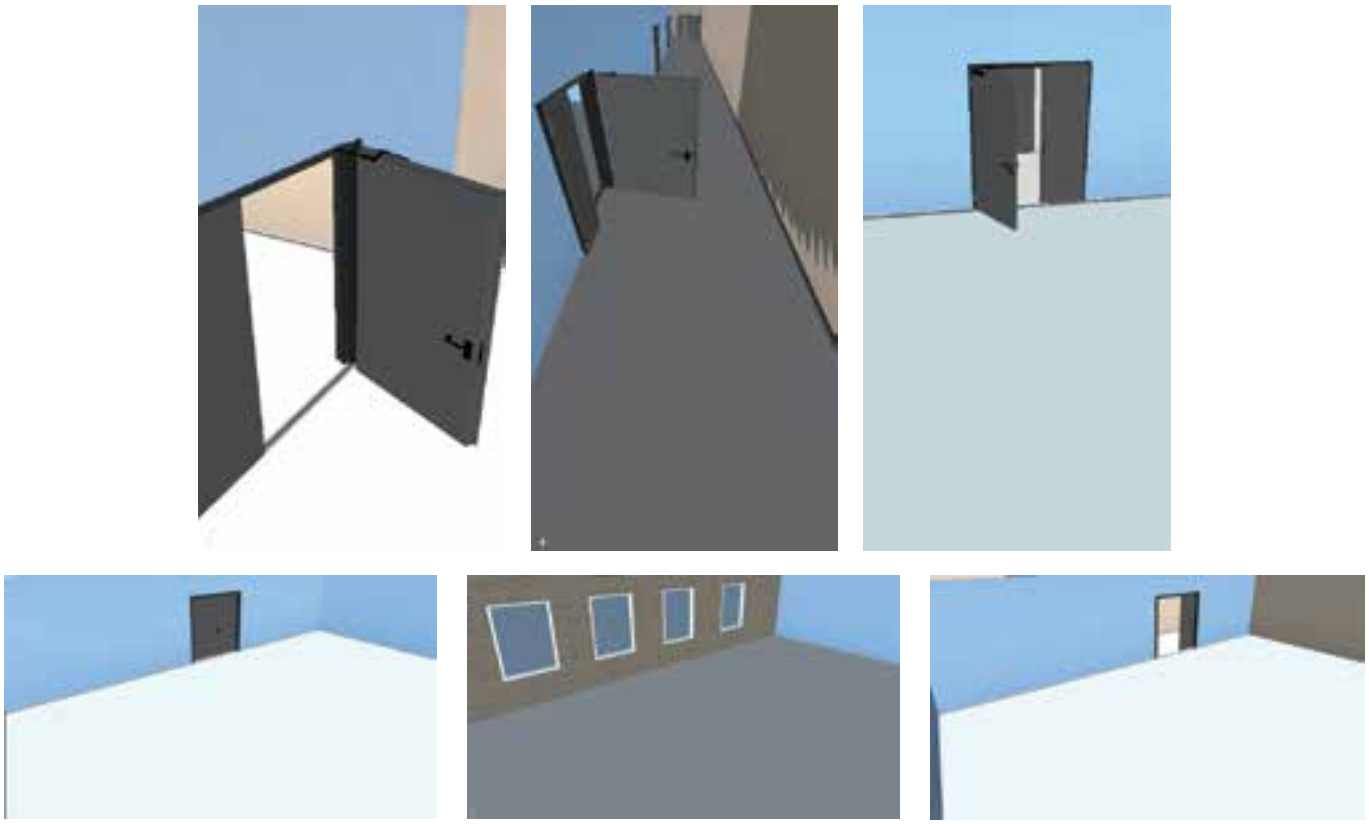


Рис. 16.1. Служебные помещения особой важности. Предполагаемое изображение с видеокамерОсновы построения сети передачи данных, системы сбора, обработки и хранения информации

ГЛАВА
5.5.
ОСНОВЫ ПОСТРОЕНИЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ, СИСТЕМЫ СБОРА, ОБРАБОТКИ И ХРАНЕНИЯ ИНФОРМАЦИИ

Система хранения данных

При построении систем видеонаблюдения одну из основных ролей играет система хранения данных. Выбор типа зависит от поставленных задач, количества подключаемых камер, длительности архива и требований к дополнительным функциям. В пункте 5.5.1 приведены общие требования, которым необходимо соответствовать согласно постановлению об антитеррористической защите:

5.5.1.
РЕЖИМЫ ЗАПИСИ:

1. непрерывная видеозапись в реальном времени;
2. видеозапись по детектору движения, сигналу от видеоаналитики, сигналу на внешних входах видеокамеры (срабатыванию охранных извещателей), видеозапись по расписанию с возможностью выбора режимов перечисленных в п/п. 1 и 2;
3. видеозапись в архив с исходным разрешением и алгоритмом сжатия с параметрами алгоритма сжатия H.264/H.265, информация о расчете архива с различным разрешением и алгоритмами сжатия приведена в главе 6.2;
4. глубина архива на срок не менее 30 суток с разграничением полномочий доступа к архиву;
5. возможность переносить на внешние носители видеофрагменты с проверкой подлинности записи, возможность конвертации;
6. в режиме записи отдельных фрагментов или видеокадров новое видеоизображение должно записываться взамен более старого, с учетом срока его хранения.

ПРИМЕЧАНИЕ: *Помимо данных режимов необходимо обратить внимание на другие характеристики, которые напрямую влияют на объем архива, качество изображения, возможность масштабируемости, отказоустойчивость и функционирование системы.*

5.5.2.
АЛГОРИТМЫ СЖАТИЯ

В современных системах видеонаблюдения применяются следующие алгоритмы сжатия: H.264/H.265 и MJPEG.

H.264/H.265

Особенности H.264/H.265 – лицензируемый стандарт сжатия видео, предназначенный для достижения высокой степени сжатия видеопотока при сохранении высокого качества. В основе лежит запись сочетаний опорного кадра I и разностного сигнала P.

- При кодировании применяется подход внутри- и межкадрового (Intra-/Inter-) предсказания и двумерного кодирования с преобразованием.
- H.264/H.265-потоки состоят из I-кадров и P-кадров.
- Из I-кадров можно восстановить оригинальное изображение, а из P-кадров – нет.
- P-кадр гораздо меньше, чем I-кадр.
- H.265 отличается от H.264 эффективностью сжатия. Кодек H.265 экономит около 50 % битрейта при том же качестве кодирования, но требует больше вычислительных ресурсов для кодирования/декодирования.
- Использование дополнительных технологий на основе H.264/H.265 (например, SmartCoding) ведет к снижению нагрузки на сетевую инфраструктуру и уменьшает объем данных на жестких дисках при сохранении высокого качества изображения.

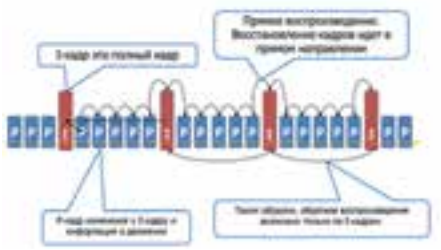


Рис. 17

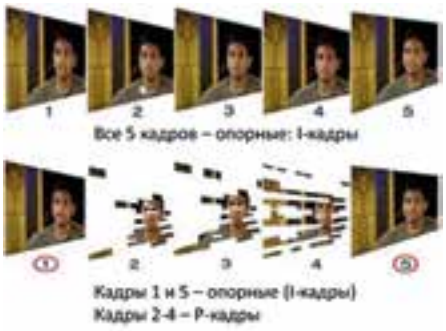


Рис. 18

MJPEG

Ведется запись каждого кадра, а не разностного сигнала предсказания, как в H.264/H.265. Данный алгоритм малоэффективен при статических сценах, когда динамики и изменений в кадре нет, а информация все равно записывается. Это существенно увеличивает объем архива.

5.5.3.
ВЫБОР ТИПА ОБОРУДОВАНИЯ ХРАНЕНИЯ ДАННЫХ

Видеорегистратор (NVR Stand Alone)

Выбор в пользу данного носителя оправдан, если не требуется интеграции со сторонним оборудованием. Данная система характеризуется простым обслуживанием, так как нет необходимости устанавливать дополнительное программное обеспечение. Также она более эффективна, если надо исключить компьютер из системы записи. Данный вариант подразумевает хранение видеоинформации на NVR.

Типовая схема построения системы приведена ниже:

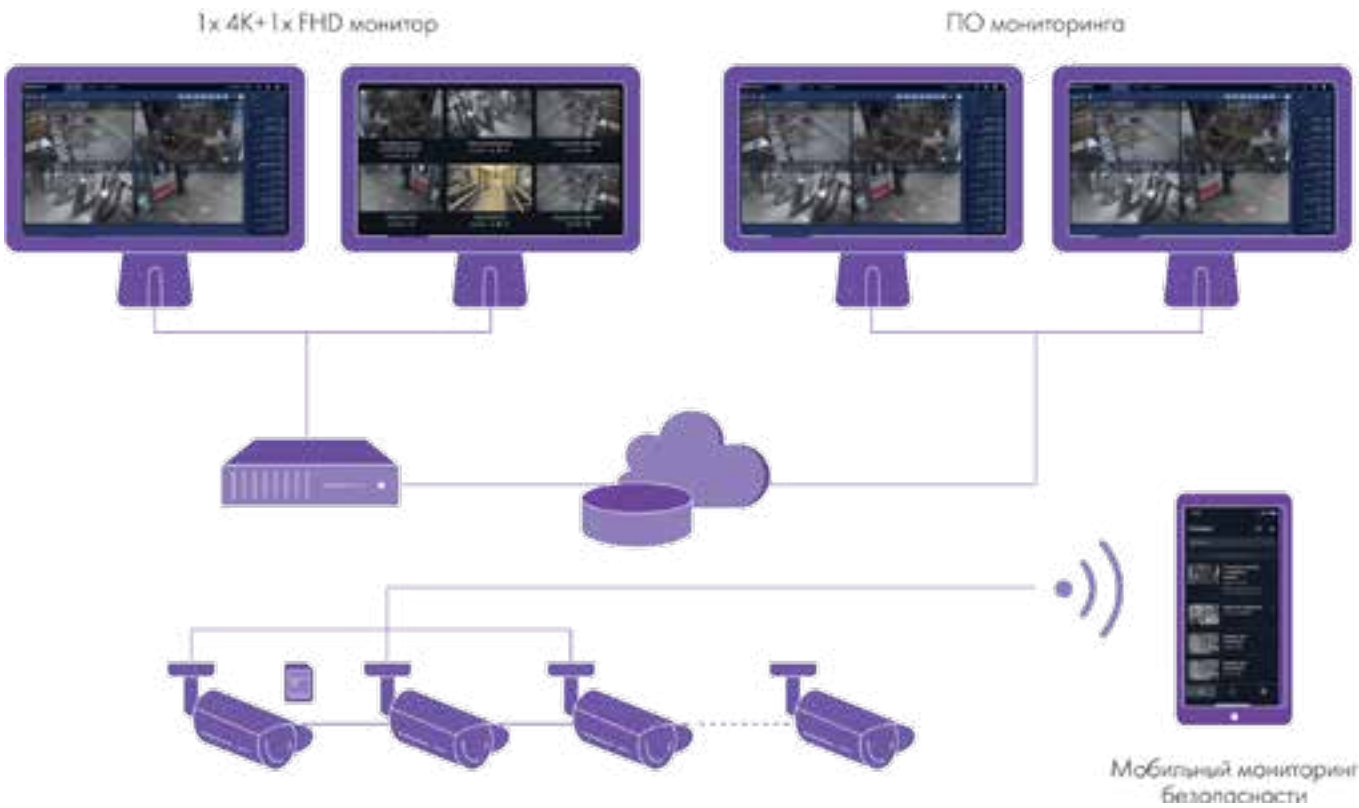


Рис. 19. Система на базе сетевых рекордеров и ПО мониторинга

Видеосервер

Используется при необходимости:

- поддержки камер стороннего производителя;
- подключения плагинов видеоаналитики (распознавание номеров, лиц, ТС и др.);
- интеграции с другими системами (СКУД, ОПС, пр.);
- универсальной масштабируемости.

ПРИМЕЧАНИЕ: *При использовании видеосервера существует несколько вариантов систем локального хранения данных.*

ВАЖНО! ***При расчете объема архива необходимо обращаться к официальным калькуляторам того вендора, чье программное обеспечение будет использовано.***

Некоторые виды реализации СХД на базе IP-серверов:

- На жесткие диски самого IP-сервера. Количество HDD ограничено количеством разъемов, поддерживаемых материнской платой.
- Система NAS, подключенная к ЛВС.
- JBOD, подключенная к ЛВС и поддерживаемая используемым программным обеспечением.

Последних два варианта имеет смысл применять в случае большого архива, который невозможно реализовать на базе IP-сервера.

Типовая схема построения системы приведена ниже:

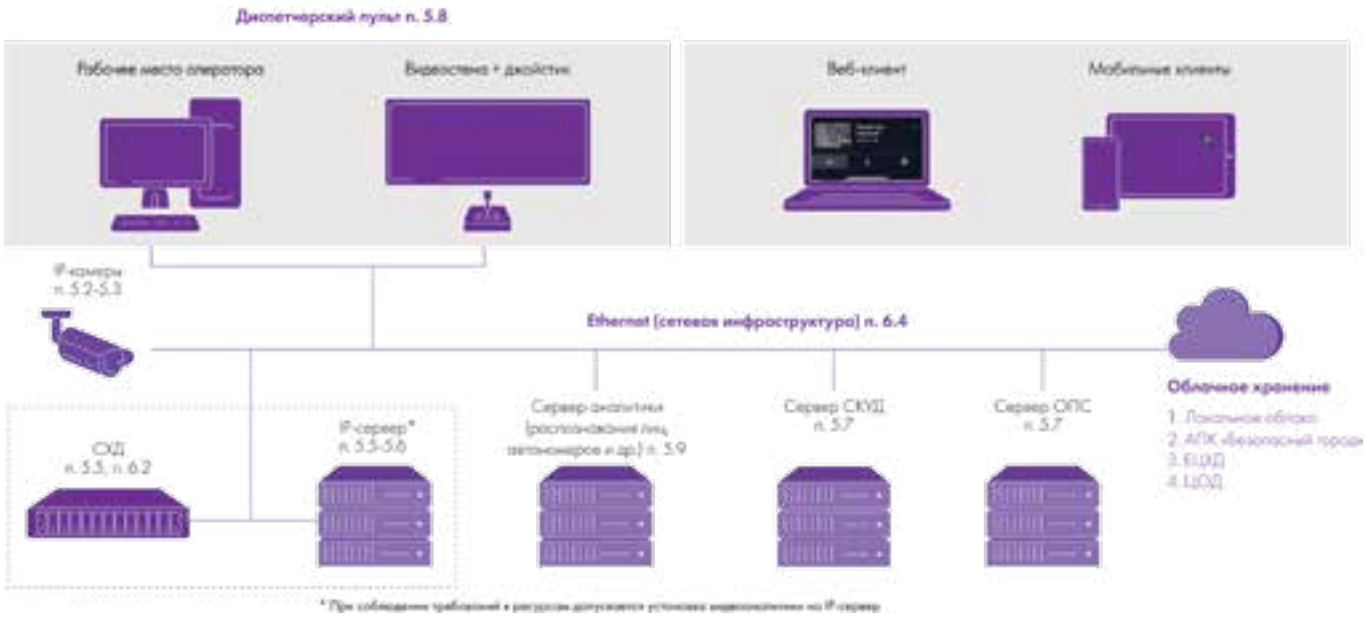


Рис. 20. Система на базе сервера (показана потенциальная возможность интеграции различных систем)

Любая из представленных схем может быть реализована с облачным хранением, например локальным облаком, АПК «Безопасный город», ЕЦХД, ЦОД, расположенным в РФ.

ВЫВОД:
Выбор той или иной системы должен производиться, учитывая как текущие требования, так и требования, которые могут возникнуть в ближайшем будущем. Вне зависимости от этого приоритетным алгоритмом сжатия будет H.265 из-за существенной экономии пространства на HDD и меньших требований к ЛВС.

ОРГАНИЗАЦИЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ (ЛВС)

Сеть передачи данных или локально-вычислительная сеть (ЛВС) играет важнейшую роль в составе современных систем безопасности. Широкое распространение унифицированных протоколов передачи данных привело к использованию сетей передачи данных в качестве основного способа связи между устройствами в системе видеонаблюдения. К ЛВС, используемым в составе систем видеонаблюдения, предъявляются повышенные требования по защищенности и отказоустойчивости.

Рассмотрим основные свойства отказоустойчивой ЛВС:

1. Топология сети с резервированием

Топология – способ соединения коммутационных устройств между собой. Отказоустойчивость различных типов архитектуры ЛВС зависит от избыточности связей и дублирования сетевых устройств.

Отсутствие избыточных связей между коммутаторами может привести к обрывам связи и нарушению работы всей сети в результате отсутствия альтернативных маршрутов передачи данных.

Увеличение количества линий связи и дублирование устройств позволяет обеспечить резервирование каналов связи и повысить производительность сети за счет распределения нагрузки и расширенной сетевой инфраструктуры.

Наиболее распространенной схемой на сегодняшний день является «звезда». Данная топология предполагает разделение всей системы на сегменты и подключение устройств к одному коммутатору внутри сегмента. Данная схема обеспечивает частичное резервирование без необходимости увеличения ресурсов ЛВС.

В случае отказа одного оконечного коммутатора произойдет отключение только одного блока системы, остальные части не будут затронуты.

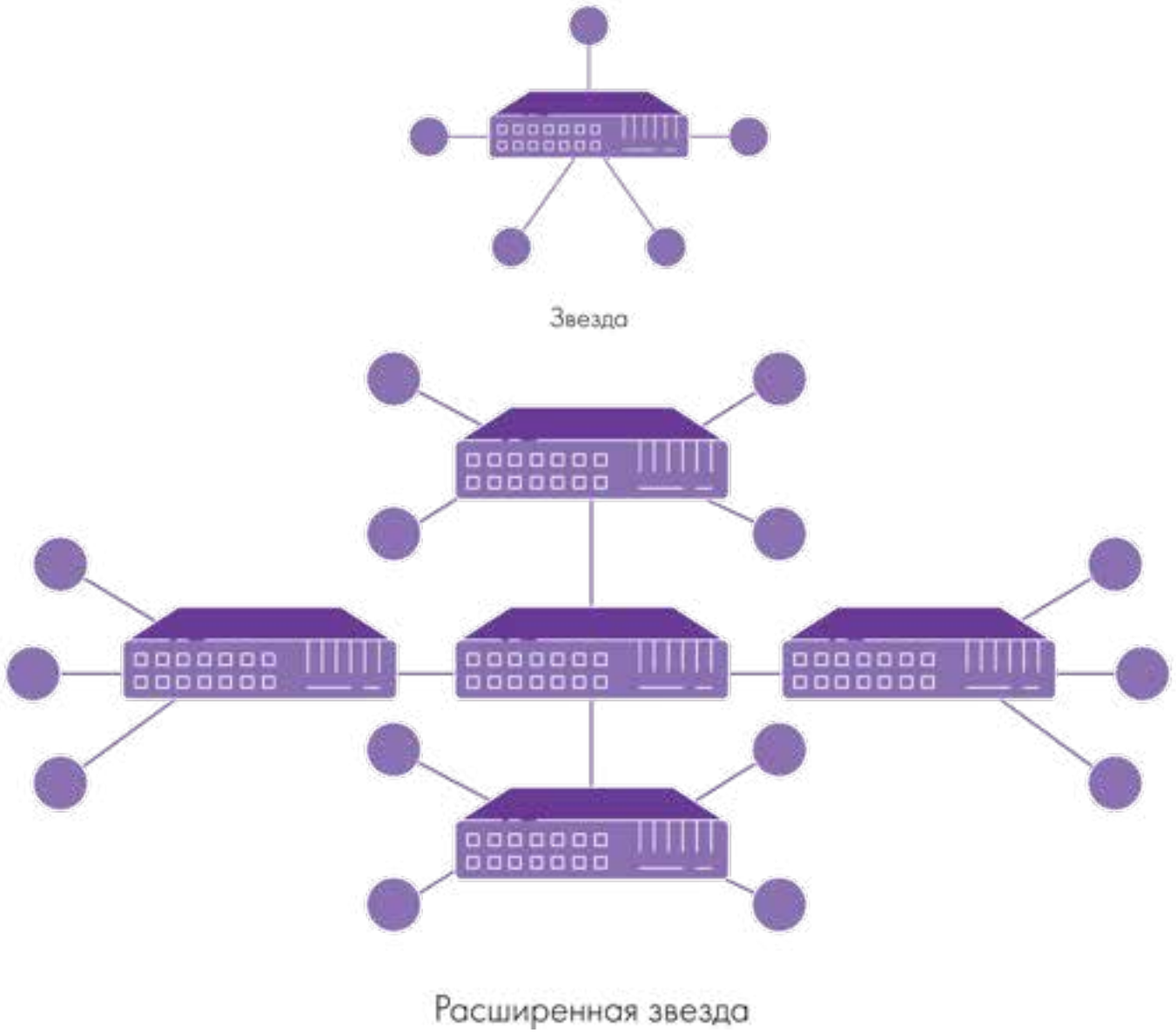


Рис. 21. Топология типа «звезда»

Помимо топологии «звезда» сохранить работоспособность сети при единичном обрыве возможно, используя кольцевое соединение коммутационных устройств. Внутри кольца каждый коммутатор подключается к соседним с обеих сторон, создавая петлю. Данные перемещаются от узла к узлу, причем каждый из них на своем пути обрабатывает каждый пакет. Это дает преимущество добавления отказоустойчивости, но при этом необходимо использовать протокол Spanning Tree Protocol (STP) или специальный кольцевой протокол Ethernet Protection Switching Rings (EPSR), чтобы предотвратить появление широковещательных штормов, так как стандарт Ethernet предусматривает только древовидную топологию и не допускает кольцевых, приводящих к зацикливанию пакетов.

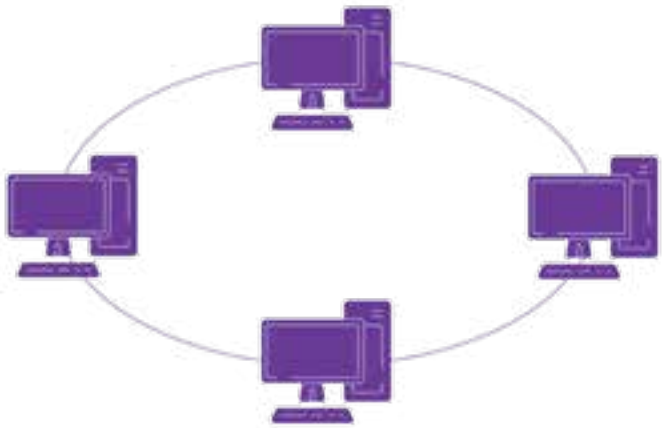


Рис. 22. Топология типа «кольцо»

При необходимости для обеспечения полной отказоустойчивости возможно применение ячеистой топологии (каждый с каждым). Данная схема подразумевает соединение всех устройств между собой с автоматическим переключением маршрута передачи данных при отказе одного из устройств. Использование ячеистой топологии требует значительного увеличения оборудования и кабельных линий.

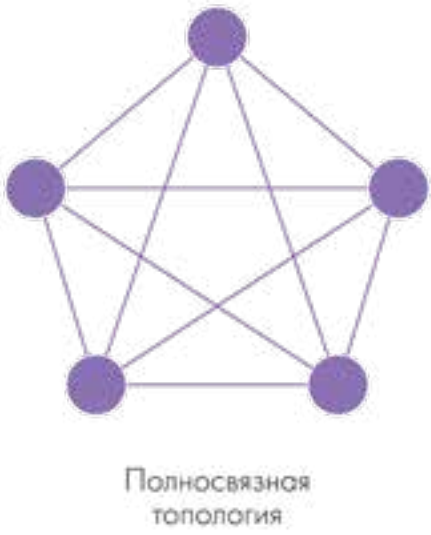


Рис. 23. Ячеистая, или полносвязная, топология

ВАЖНО! ***Схема ЛВС видеонаблюдения не должна содержать последовательных соединений коммутаторов в единую цепочку без обеспечения резервирования каналов связи. В случае отказа одного из узлов сети передача данных к последующим устройствам невозможна и сеть становится крайне уязвимой к неисправностям.***

Рис. 24. Ошибочная топология с последовательным соединением

2. Оценка пропускной способности сети и максимального потока с видеокамер

При построении сети для систем IP-видеонаблюдения важными показателями является величина максимального потока, создаваемого всеми видеокамерами системы и пропускная способность (величина максимального потока, который способна транслировать сеть). Проектирование сети системы IP-видеонаблюдения начинают с нахождения максимальных информационных потоков, создаваемых всеми видеокамерами системы.

Среднее значение потока от каждой камеры зависит от ее разрешающей способности, от используемых кодеков сжатия, выбранной частоты кадров, интенсивности движения в поле зрения камеры, наличия видеоаналитики. Для определения скорости информационного потока от каждой камеры рекомендуется использовать специализированные калькуляторы, размещенные на сайте производителя.

Пропускная способность сети определяется выбранной средой передачи сигнала. Наиболее популярным видом среды передачи данных на небольшие расстояния (до 100 м) становится неэкранированная витая пара (UTP), которая включена практически во все современные стандарты и технологии локальных сетей и обеспечивает пропускную способность до 100 Мбит/с. Экранированная витая пара (STP категории 6) позволяет увеличить пропускную способность до 1000 Мбит/с.

Оптоволоконный кабель широко применяется как для построения локальных связей, так и для образования магистралей глобальных сетей. Оптоволоконный кабель может обеспечить очень высокую пропускную способность канала (до нескольких Тбит/с) и передачу на значительные расстояния (до нескольких десятков километров без промежуточного усиления сигнала).

ВАЖНО! ***Типичные ошибки при расчете сетей передачи данных:***

- ***Превышение показателя максимальной загрузки портов коммутатора. При загрузке всех портов коммутатора общий информа-***

ционный поток не должен превышать значение максимальной пропускной способности коммутатора, в противном случае возможно возникновение задержек при передаче видеоданных и задержка работы системы хранения данных.

• Резкое увеличение значений потока с видеокамер. Изменение внешних условий, например засветка или увеличение движения в кадре, приводит к повышению потоков, получаемых с видеокамер. Для увеличения надежности работы сети в части предотвращения непредвиденных перегрузок от изменения интенсивности движения перед видеокамерами, для расчетов целесообразно увеличить на 25–30 % общее полученное значение скорости потока.

• Превышение максимальной длины среды передачи.

3. Комплекс мер по информационной защите

Современные IP-сети систем видеонаблюдения могут быть подвержены угрозам информационной безопасности, таким как:

- утрата, подмена и несанкционированный просмотр видеоархива;
- перехват, изменение данных при передаче;
- нарушение стабильной передачи по каналу;
- несанкционированный доступ к видеоизображению и конфигурации системы
- вредоносное ПО (вирусы и т. п.).

Для противодействия указанным угрозам необходимо применять комплекс мер по информационной безопасности. Конечные требования по защите информации в системах видеонаблюдения рекомендуется определять на стадии разработки проектной документации с привлечением специалистов в области информационной безопасности.

Основной набор мероприятий по защите информации в сети видеонаблюдения должен включать:

1. Встроенную защиту программного обеспечения видеонаблюдения (предусмотренную производителем), например разграничение прав пользователей, установка паролей, шифрование трафика.
2. Защиту сети передачи данных, коммутационного оборудования. В числе мер рекомендуется выполнять разделение сети на VLAN, фильтрацию по MAC-адресам, блокировку неиспользуемых портов сетевых коммутаторов.
3. Внешнюю защиту от вредоносного ПО, разграничение доступа к интерфейсу ОС.
4. Ограничение доступа посторонних лиц к коммутационному оборудованию.

Комплекс мер по защите системы видеонаблюдения должен разрабатываться с учетом структуры построения сети связи. При отсутствии внешних подключений (закрытая сеть) достаточно использования минимального набора основных мероприятий по защите, в случае интеграции с внешними системами или при использовании канала передачи между сегментами сети посредством внешних неконтролируемых сетей (интернет) информационная защита всех элементов системы (канал связи, коммутаторы внешнего доступа, клиентское оборудование) является обязательной.

Вопросы, связанные с информационной защитой, нередко остаются без должного внимания проектировщиков, и основная задача по разработке мер защиты от угроз кибербезопасности возлагается на конечных пользователей систем.

ВАЖНО! ***Информационная защита систем видеонаблюдения – это непрерывный процесс, настоятельно рекомендуется проводить мероприятия по регулярной замене паролей, созданию резервных копий и установке актуальных версий программного обеспечения.***

ВЫВОДЫ:

1. Сеть передачи данных является одной из основных частей систем видеонаблюдения, к которой предъявляются повышенные требования по защищенности и отказоустойчивости.

2. Отказоустойчивость ЛВС достигается путем правильных расчетов потоков данных от всех устройств и выбором соответствующей топологии сети с достаточной избыточностью соединений.

3. Защищенность ЛВС обеспечивается выполнением комплекса мер по информационной защите.

ГЛАВА 5.6. ЛИЦЕНЗИРОВАНИЕ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА. ВИДЫ ЛИЦЕНЗИЙ

В зависимости от типа системы видеонаблюдения, количества видеокамер, объема системы хранения данных, а также уровня интеграции с другими системами безопасности и жизнеобеспечения возможны различные комбинации лицензий, предъявляемых производителями программного обеспечения.

По сроку действия лицензии подразделяются на **бессрочные и с ограниченным сроком действия**.

Основные типы лицензий, применяемые в системах видеонаблюдения:

- Лицензии на основное оборудование:
  - ядро системы (экземпляр программного обеспечения) / сервер / регистратор;
  - канал видеонаблюдения.

- Лицензии на АРМы и мониторы:
  - оператор,
  - администратор,
  - пульт управления (джойстик),
  - монитор видеостены.
- Лицензии на видеоаналитику:
  - функционал видеоаналитики на камере;
  - поиск в архиве.
- Лицензии на резервирование:
  - резервный сервер записи/управления.
- Лицензии по интеграции и подключению стороннего оборудования:
  - enterprise – расширение и объединение систем;
  - интеграция подсистем безопасности;
  - иные лицензии интеграции.
- Способы лицензионной защиты:
  - аппаратный USB-ключ: может быть перенесен на другой ПК;
  - программный ключ: привязывается к определенному ПК и может быть перенесен только при содействии производителя программного обеспечения.

5.6.1. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА VS СЕРВИСНАЯ ПОДДЕРЖКА

В процессе использования программного обеспечения неизбежно возникают вопросы по его работе, возможным неполадкам, обновлению, расширению функциональных возможностей или просто масштабированию существующего технического решения.

Для успешного разрешения этих вопросов важно понимать, что входит в обязательства производителя в рамках гарантии, а что может быть выполнено только в рамках отдельного сервисного контракта на техническое обслуживание.

Итак, **гарантия** – это обязательство производителя устранить возникшие по его вине неполадки в работе программного обеспечения. Другими словами, в течение гарантийного срока на ПО разработчик обязан в согласованный срок предоставить исправно работающую версию программного обеспечения. При этом необходимо, чтобы были соблюдены следующие требования:

- наличие сбоя имеет документальное подтверждение;
- имеется подтверждение того, что сбой произошел по вине разработчика;
- предоставлен алгоритм действий пользователя в системе, вызывающих данную ошибку;
- эксплуатация программного обеспечения велась корректно в соответствии с инструкцией;
- не имело место самостоятельное вмешательство пользователя в устройство программного обеспечения;
- претензия пользователя соответствует заявленным характеристикам программного продукта.

При этом бремя сбора и предоставления указанных сведений и материалов лежит на пользователе программного обеспечения. Также необходимо иметь ввиду, что в соответствии с действующим законодательством РФ, если в договоре поставки (или лицензионном договоре) не указан гарантийный срок, то покупатель вправе будет предъявить требования производителю в связи с недостатками, обнаруженными в течение разумного срока, но в пределах двух лет с момента передачи товара (п. 2 ст. 477 ГК РФ).

ПРИМЕЧАНИЕ: ***Производитель вправе устанавливать иной гарантийный срок, не противоречащий положениям ГК РФ, на выпускаемое программное обеспечение. Максимальный срок устранения выявленных неполадок в работе программного обеспечения при этом составляет 45 дней.***

ВАЖНО! ***Гарантия производителя ограничивается именно исправлением ошибок в том экземпляре программного обеспечения, который приобрел покупатель. Технические консультации по вопросам использования ПО, получение программных обновлений, обеспечение совместимости с другими программами пользователя или специальными аппаратными средствами и многие другие вопросы – не входят в объем гарантийных обязательств.***

Безусловно, компании – производители программного обеспечения, дорожащие своими клиентами и репутацией, стараются выявить и исправить очевидные дефекты в своем ПО, предоставляют бесплатные обновления в рамках текущей версии продукта, однако большинство вопросов предлагается решать самостоятельно, пользуясь информацией, содержащейся в эксплуатационной документации на ПО, базе знаний и электронных форумах на сайте производителя или авторизованных партнеров.

Как правило, в объеме гарантийных обязательств предоставляется следующий перечень услуг:

- анализ выявленных и подтвержденных ошибок в программном обеспечении;
- исправление дефектов программного обеспечения и предоставление обновлений программного обеспечения с устраненными выявленными ошибками в виде хотфиксов, патчей или целиком сборок ПО;
- предоставление удаленного доступа к информационной системе контроля выполнения запросов пользователей.

5.6.2. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА/СЕРВИСНАЯ ПОДДЕРЖКА/СОПРОВОЖДЕНИЕ ПО – УСЛУГИ, ПОСРЕДСТВОМ КОТОРЫХ ПРОИЗВОДИТЕЛЬ ИЛИ АВТОРИЗОВАННЫЙ ПАРТНЕР ОБЕСПЕЧИВАЮТ ПОМОЩЬ ПОЛЬЗОВАТЕЛЯМ ПРИ РАБОТЕ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Цель технической поддержки – сопровождение пользователей в решении возникающих конкретных проблем с использованием ПО, обучением, индивидуальной настройкой или другими задачами в части использования как самого программного обеспечения, так и всего программно-аппаратного комплекса, включающего в свой состав данное ПО, в соответствии с соглашением об уровне сервиса (SLA).

Главное отличие сервисной поддержки от гарантийного обязательства в том, что в рамках сервисной техподдержки производитель обязуется устранять любые недочеты, в том числе возникшие по вине пользователя, в строго оговоренные сроки, предусмотренные SLA.

Техническая поддержка может включать следующие виды услуг:

- предоставление обновлений программного обеспечения в течение оговоренного срока или линейки версий ПО, установка обновлений ПО на оборудовании пользователя;
- прием и обработка запросов пользователя на получение консультаций и устранения ошибок в ПО, запросов на улучшение ПО или разработки новой функциональности;
- консультации и обучение пользователей работе с продуктом, конфигурирование, предоставление горячей линии для обращений пользователей;
- мониторинг работоспособности и производительности программного комплекса на оборудовании пользователя, администрирование системы заказчика в целом;
- согласованный объем человеческих ресурсов для проведения доработок программного продукта по требованию заказчика.

ВАЖНО! ***Сервисная поддержка, в отличие от гарантийных обязательств, является платной услугой, стоимость которой во многом определяется параметрами соглашения об уровне сервиса (SLA): временем реакции на обращение пользователя, временем диагностики и устранения неисправностей, объемом профилактических и регламентных работ, режимом работы службы технической поддержки, соглашением о выезде специалистов производителя или сервисной компании для осуществления аварийно-восстановительных работ на объектах заказчика.***

5.6.3. СРОК ЖИЗНИ ПО. ВЕРСИОННОСТЬ. ОБНОВЛЕНИЯ

Несмотря на то что программное обеспечение зачастую продается по лицензионному договору с бессрочным правом использования, на практике реализовать это право представляется довольно затруднительным.

Во-первых, любой продукт, в том числе и программное обеспечение, имеет ограниченный жизненный цикл, который устанавливается производителем и зависит от многих факторов, включая технологическое совершенствование аппаратного обеспечения, появление новых технологий, средств разработки, алгоритмов машинного обучения, рыночной конъюнктуры и прочего. По окончании этого жизненного цикла программное обеспечение сначала перестает продаваться, а затем прекращается и сервисная поддержка производителем. При этом пользователь ПО, приобретший право бессрочного использования, сохраняет это право именно на приобретенный экземпляр программного обеспечения, даже когда сам программный продукт более не поддерживается производителем.

ВАЖНО! ***Использование продуктов, поддержка которых прекращена производителем, несет в себе множество рисков и является нежелательной для критически важных объектов или систем.***

Производство программного обеспечения связано с применением и реализацией тех или иных технологий хранения и обработки данных, сред выполнения машинного кода, фреймворков, подходов к архитектуре и разработке ПО, алгоритмов, аппаратного обеспечения и микрокодов. Эволюционное развитие техники делает сегодня нецелесообразным, а иногда и вовсе невозможным использование программного обеспечения, ориентированного на технологический стек прошлых лет. Для адаптации к таким эволюционным циклам производители ПО используют механизм версионности программных продуктов.

В рамках основной текущей версии выпускаемого программного обеспечения, как правило, сохраняются базовые функциональные возможности, совместимость с аппаратными платформами, используемый набор технологий, актуальных на момент выпуска. Для основной версии в течение жизненного цикла ПО регулярно выпускаются программные обновления, учитывающие появление новых аппаратных средств, исправление ошибок, добавление функциональных возможностей. Когда развитие продукта в рамках подходов и технологий, применяемых в текущей версии программного продукта, становится нецелесообразным, выпускается новая версия ПО.

ПРИМЕЧАНИЕ: ***Как правило, для пользователя переход на новую версию ПО доступен только через повторное приобретение лицензии или через платную программу миграции.***

Во-вторых, сама организация, приобретая программное обеспечение, определяет срок его полезного использования. Как правило, для ПО, полученного по лицензионному договору с бессрочным правом пользования, устанавливается предполагаемый срок использования программ для ЭВМ с учетом срока, установленного ГК РФ (не менее 5 лет, п. 4 ст. 1235 ГК РФ). В период установленного срока полезного использования в соответствии с принятой учетной политикой в организации и нормами законодательства РФ, в бухгалтерском и налоговом учете отражаются расходы на приобретение ПО.

В результате окончания срока полезного использования организации следует определиться, как поступить с полностью самортизированным основным средством: ликвидировать его или продать, отремонтировать или реконструировать (модернизировать).

Как правило, моральный и физический износ программного обеспечения настолько велик, что его следует ликвидировать.

5.6.4. АДАПТАЦИЯ. МОДИФИКАЦИЯ. ЗАКАЗНАЯ ДОРАБОТКА ПО

На практике часто случается так, что программный продукт не в полной мере отвечает потребностям заказчика в части функционального наполнения или совместимости с уже имеющимся оборудованием. Гражданский кодекс в этой части выделяет два способа внесения изменений в существующее произведение – адаптацию и модификацию.

Согласно норме закона «***адаптация***, *то есть внесение изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя*», не признается переработкой программного обеспечения. Пользователю, правомерно владеющему экземпляром программы, предоставлено право на осуществление адаптации при условии ненарушения остальных правил пользования программным обеспечением, а именно: получения исходного кода программы путем дизассемблирования, внесения в него изменений, вскрывания используемых технологий и т. п. По сути, соблюдение данных условий позволяет проводить адаптацию программных продуктов путем конфигурирования экземпляра ПО на оборудовании заказчика разрешенными правообладателем способами.

Зачастую правообладатели в явном виде запрещают пользователям и адаптацию программных продуктов во избежание необходимости нести гарантийные обязательства по программному обеспечению, используемому в среде или в конфигурации, для которой не проводилось надлежащее тестирование.

Что касается **модификации** программного обеспечения, то, согласно подп. 9 п. 2 ст. 1270 ГК РФ, «под переработкой (модификацией) программы для ЭВМ или базы данных понимаются любые их изменения», а само модифицированное ПО будет являться самостоятельным производным произведением. Исходя из буквального прочтения норм Гражданского кодекса, можно заключить, что, получив разрешение от правообладателя на модификацию программного обеспечения, «автор модификации» вправе распоряжаться программой как новым произведением как его полноправный правообладатель. Единственное требование для такого автора модифицированной программы будет заключаться в указании авторов исходной программы.

В этой связи предоставление разрешения на модификацию программы для ЭВМ – явление крайне редкое, если речь не идет о передаче исключительных прав или работе с так называемым открытым программным обеспечением. Поэтому доработки программы под нужды пользователя могут быть выполнены либо самим правообладателем ПО, либо же реализованы сторонними разработчиками в виде плагинов или дополнительных модулей, если архитектура программы позволяет это.

При заключении договора с правообладателем на заказную доработку ПО, однако, стоит иметь ввиду, что по умолчанию в силу положений ГК РФ исключительное право на программное обеспечение принадлежит заказчику. Если же стороны с этим не согласны, то у них должно быть и техническое задание, в котором предусмотрен объем изменений, вносимых в компьютерную программу, и условия договора о распределении прав на модифицированную программу. На практике же заказная разработка редко затрагивает изменение всей программы и бывает выражена в виде разработки специальных программных модулей под нужды заказчика таких доработок.

ВАЖНО! ***Как в случае оформления доработок в виде модифицированной сборки программы, так и специализированных плагинов или программных модулей, производитель не несет обязательств по совместимости будущих версий своего ПО с произведенными под конкретного пользователя доработками, поскольку модифицированная программа является новым произведением, и взаимоотношения правообладателя и пользователя должны регулироваться отдельным лицензионным договором уже на новое произведение.***

5.6.5. ВОЗМОЖНОСТИ МОДЕРНИЗАЦИИ

Непрерывное развитие цифровых технологий приводит к быстрому моральному устареванию технических устройств. Системы видеонаблюдения стремительно модернизировались последние десятки лет. Переход от аналогового телевидения к цифровому – один из наиболее значимых этапов развития всей сферы видеонаблюдения.

Этап замены кабельных линий при модернизации является наиболее трудоемким, особенно при проведении работ на объектах культурного наследия. Технологии аналогового телевидения высокой четкости (HD-TVI, AHD, HD-CVI) позволяют получить изображение с разрешением, достаточным для решения большей части основных задач видеонаблюдения. Указанные технологии используют передачу данных по коаксиальным линиям связи, следовательно при модернизации системы прокладка кабельных линий не требуется. Следует отметить, что данные технологии предъявляют высокие требования к качеству соединения между аналоговой видеокамерой высокой четкости и преобразователем/видеокодером. На практике качество старых коаксиальных линий не всегда соответствует этим требованиям из-за наличия множественных соединений и повреждений, что накладывает ограничения на применение указанных технологий для модернизации систем.

ВАЖНО! ***В целях упрощения эксплуатации систем видеонаблюдения рекомендуется соблюдать все требования по техническому обслуживанию систем, учитывать сроки технической поддержки оборудования, обеспечить необходимый набор запасных частей и расходных материалов на весь прогнозируемый срок полезной эксплуатации, а также предусматривать решения по модернизации систем видеонаблюдения на стадии проектирования.***

ВЫВОДЫ:

- ***Политика лицензирования программно-аппаратного комплекса систем видеонаблюдения устанавливается производителями оборудования и ПО.***
- ***На стадии разработки и проектирования рекомендуется закладывать все лицензии с учетом возможного расширения системы.***
- ***Если вы планируете создавать комплексную систему безопасности, используете в составе технического решения программные продукты с индивидуальными доработками и не имеете достаточно квалифицированных специалистов в штате, имеет смысл рассмотреть заключение сервисного контракта на сопровождение приобретаемого программного обеспечения.***
- ***Приобретая бессрочное право на пользование программным обеспечением, не следует рассчитывать на пожизненные бесплатные обновления от производителя – в большинстве случаев они доступны только в рамках текущей версии продукта, а за переход на новую версию продукта придется доплачивать.***
- ***Заказные доработки программного обеспечения, как правило, будут связаны с необходимостью заключения сервисного контракта на техническое сопровождение создаваемой системы, чтобы обеспечить последующую доступность обновлений программного обеспечения и их совместимость с произведенными доработками.***

ГЛАВА 5.7. ПРИНЦИПЫ ИНТЕГРАЦИИ С ПОДСИСТЕМАМИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ, АВТОМАТИЗАЦИИ ЗДАНИЯ И ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Общие принципы интеграции подсистем безопасности

Видеонаблюдение может использоваться в качестве отдельного блока в составе систем жизнеобеспечения зданий, однако наибольшая эффективность достигается при использовании видеонаблюдения совместно с другими системами в качестве единой интегрированной системы безопасности объекта.

Целью интеграции видеонаблюдения с системами безопасности и жизнеобеспечения является:

- обеспечение оперативной работы персонала;
- снижение времени реакции на события, особенно для крупных объектов с большим количеством оборудования;
- снижение количества диспетчерского персонала, необходимого для работы за пультом;
- сокращение времени поиска архивной информации для разбора ситуаций, имевших место в прошлом.

В процессе интеграции с инженерно-техническими средствами безопасности и инженерными системами решаются следующие задачи:

- непрерывный автоматический сбор и обработка информации от внешних систем;
- выявление и верификация угроз безопасности из разных систем;
- корреляция между событиями безопасности из различных систем;
- использование единых планов и схем помещений или картографических подложек для всех интегрируемых систем;
- долговременное хранение информации об инцидентах с возможностью их последующего постанализа;
- предоставление отчетов по полученным событиям безопасности и созданным инцидентам;
- автоматизированный контроль работы внешних систем.

Интеграция возможна на уровне аппаратного или программного обеспечения или комбинированная.

Под аппаратной интеграцией подразумевается физическое соединение тревожных входов/выходов устройств систем жизнеобеспечения здания. Наиболее часто используется для небольших объектов с целью расширения функциональных возможностей устройств и автоматизации работы систем, а также в случаях, когда программная интеграция невозможна в силу технических ограничений систем.

В качестве примеров можно привести:

- включение лампы освещения по сигналу от извещателя охранной сигнализации;
- подключение сирены к выходу видеокамеры с функцией видеоаналитики пересечения линии. В случае когда посетитель пересекает обозначенную линию, видеокамера выдает тревогу и автоматически включается подключенная сирена;
- открытие/закрытие шлагбаума или ворот по результатам распознавания автомобильных регистрационных знаков;
- передача сигнала тревоги из пожарной сигнализации в систему диспетчеризации.

Интеграция на уровне программного обеспечения осуществляется путем объединения всех принимаемых сигналов от подключаемых инженерных систем под управлением центрального сервера в едином программном поле. Оператор ПО в таком случае работает с мнемосхемой или интерактивным планом объекта с возможностью управления всеми системами без необходимости переключения между отдельными программами.

ВАЖНО! ***Данный тип интеграции обладает значительными возможностями настройки взаимодействия систем и автоматизации управления при возникновении нештатных ситуаций.***

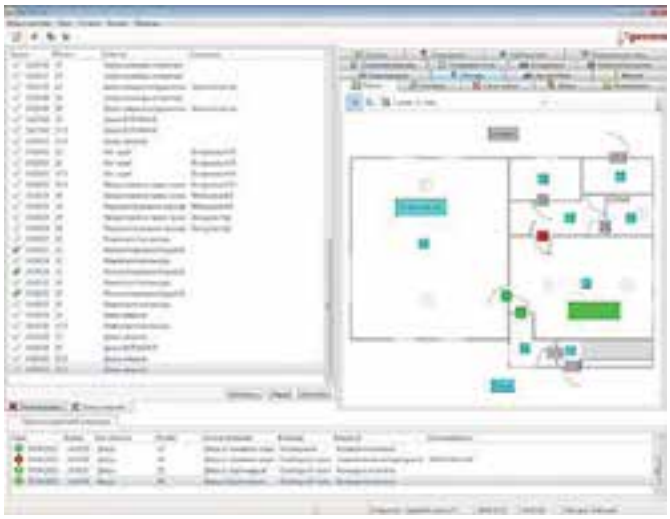


Рис. 25. Пример программно-интегрированной системы безопасности

ВАЖНО! ***При проектировании и эксплуатации программно-интегрированных систем безопасности особое внимание необходимо уделять синхронизации времени в отдельных частях комплексной системы безопасности. Отсутствие синхронизации времени приводит к ситуациям, когда при разборе происшествий тревога по одной из подсистем не подтверждается другой системой. Кроме того, синхронизация времени обеспечивает эффективные алгоритмы взаимодействия подсистем, следовательно оператор диспетчерского пульта сможет оперативно принять верное решение***.

Не менее важным аспектом является возможность автоматической синхронизации списка устройств в интегрируемой подсистеме и в центральном сервере диспетчеризации. Часто администрирование и настройка подключаемых подсистем осуществляется через программные средства самой подсистемы, вне центрального сервера управления диспетчеризацией, а иногда и вовсе за интегрируемую систему отвечает отдельное

организационное подразделение или подрядчик. В таких случаях необходимо, чтобы и сама интегрируемая подсистема, и центральный сервер управления единого программно-аппаратного комплекса имели возможность при изменении конфигурации автоматически синхронизировать списковые справочники подключенных устройств с регистрацией таких изменений.

Рекомендуется комбинировать программную и аппаратную интеграцию в зависимости от поставленных задач. Вне зависимости от типа и площади объекта культуры наиболее эффективным способом управления системами жизнеобеспечения будет являться объединение таких систем под управлением единого программно-аппаратного комплекса.

Далее рассмотрим рекомендованное возможное прикладное использование интеграции системы видеонаблюдения с другими системами безопасности, диспетчеризации и системами обеспечения жизнедеятельности объектов культуры.

СКУД (включая работников и посетителей)

- автоматический вывод изображения с ближайшей видеокамеры при нарушении режима прохода через точку под управлением СКУД;
- быстрый поиск видеоархива с маршрутом перемещения человека на основании данных СКУД;
- автоматическая блокировка карты доступа при обнаружении превышения температуры тела видеокамерой с функцией термометрии;
- использование технологии распознавания лиц для двухфакторной аутентификации (карта + лицо) при проходе через КПП или на иных рубежах контроля с повышенными требованиями по безопасности.

Охранная сигнализация

- автоматический вывод изображения с ближайшей видеокамеры для подтверждения сигнала о несанкционированном доступе от системы ОС;
- использование функций видеоаналитики в качестве детектора тревожных событий (пересечение линии, оставленный предмет, вход в запрещенную зону).

Системы противопожарной защиты

- автоматический вывод изображения с ближайшей видеокамеры для подтверждения сигнала о пожаре от системы АПС;
- контроль срабатывания системы автоматического пожаротушения при помощи видеокамер;
- контроль и управление аварийной эвакуацией людей при пожаре;
- система автоматизации и диспетчеризации зданий;
- технологическое видеонаблюдение в технических помещениях зданий и сооружений для контроля параметров систем жизнеобеспечения;
- автоматический вывод изображения с ближайшей видеокамеры для подтверждения сигнала о протечке;
- передача в систему диспетчеризации результатов измерения, полученных при помощи средств термографии.

Кассовый блок

- совмещение видеоданных и текстовой информации чеков с кассовых аппаратов;
- поиск видеоряда по заданным критериям (времени, отделу, номеру кассы, имени кассира, названию товара, типу операции, суммы чека, суммы скидки, текстовой строке).

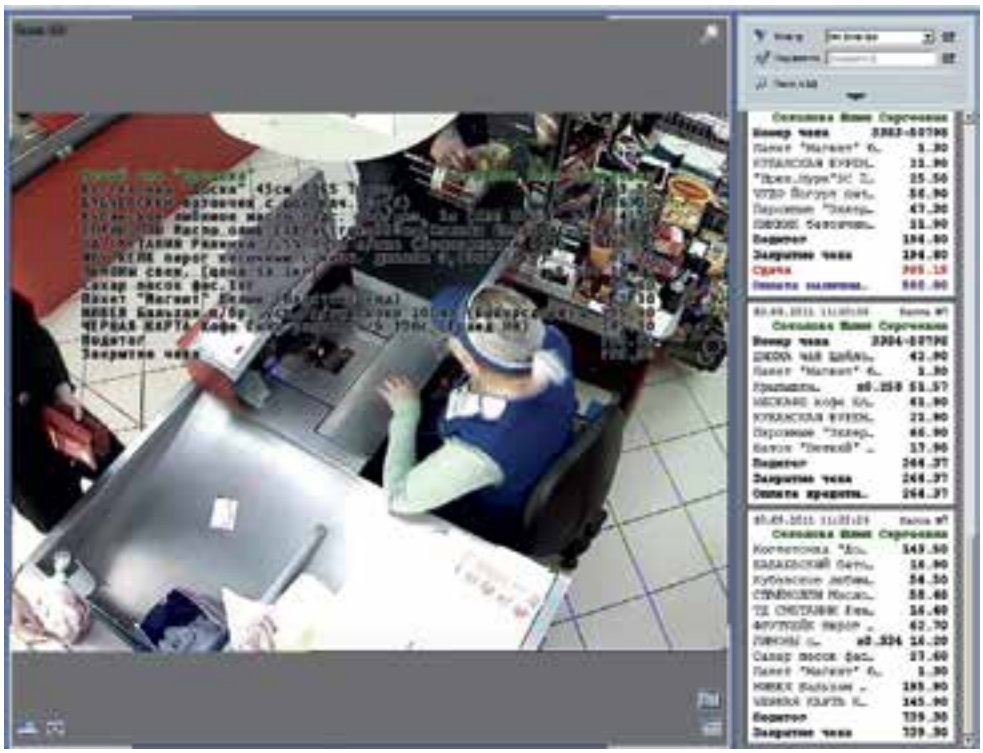


Рис. 26.
Пример интеграции видеоданных с информацией кассового чека

Система речевого оповещения

- привязка динамиков отдельной системы речевого оповещения к зоне обзора видеокамеры для передачи адресных речевых сообщений посетителям.

Досмотровое оборудование

- передача в систему видеонаблюдения изображения результатов сканирования личных вещей и багажа в рентгенотелевизионной установке;
- автоматический вывод изображения с ближайшей видеокамеры при поступлении сигнала о сработке средств обнаружения паров/следов взрывчатых веществ или металлодетекторов.

При интеграции систем безопасности и жизнеобеспечения в единый информационно-диспетчерский комплекс важно обращать внимание на возможность интегрируемых систем по передаче тех или иных сообщений и параметров этих сообщений. Рекомендованный перечень регистрируемых ситуаций и параметры передаваемых в систему диспетчеризации значений приведен в таблице ниже:

№ п/п	Инженерно-технические средства и системы	Регистрируемые ситуации и тревожные сообщения	Передаваемые значения
1.	Видеонаблюдение	Видеоизображение со всех видеокамер, вовлеченных в обеспечение безопасности. Доступ к записям видеоинформации в архиве. Экспорт записей видеоинформации из архива и хранение ее совместно с карточкой инцидента. События видеоаналитики (информация о фактах обнаружения лиц, предметов и признаков чрезвычайной ситуации с привязкой по времени). Исправность видеокамер (неисправность любой видеокамеры, восстановление работоспособности видеокамеры).	Категория события. Время фиксации. Место фиксации. Источник события.
2.	СКУД	Инцидент (выдача информации о попытках несанкционированного прохода людей (транспортных средств) на (из) охраняемого объекта в зону безопасности и/или на критический элемент). Неисправность компонентов системы.	Наименование инцидента (тревожного события). Категория события. Время фиксации. Место фиксации.
3.	АПС, ОС, ОСП	Инцидент (выдача информации о сработках датчиков/шлейфов сигнализации). Неисправность компонентов системы.	Наименование инцидента (тревожного события). Категория события. Время фиксации. Место фиксации.
4.	Технические системы и средства досмотра. Интроскопия	Обнаружение металлических предметов и органических веществ.	Время фиксации. Категория события. Проекционные теневые рентгеновские изображения, рентгеновские томографические изображения; изображения, формируемые досмотровой системой на обратнорассеянном рентгеновском излучении.
5.	Технические системы и средства досмотра. Газовый анализ	Обнаружение повышенной концентрации опасных газов.	Время фиксации. Категория события. Тип опасного газа.
6.	Технические системы и средства досмотра. Радиационный контроль	Обнаружение повышенного радиационного излучения.	Время фиксации. Категория события. Изображения, формируемые досмотровой радиометрической системой.
7.	Технические системы и средства досмотра. Зондирование нейтронами	Обнаружение взрывчатых веществ.	Время фиксации. Категория события. Тип взрывчатого вещества (данные установки зондирования «быстрыми мечеными» нейтронами).
8.	Технические системы и средства досмотра. Металлообнаружитель	Исправность средств досмотра (неисправность металлообнаружителя, восстановление работоспособности).	Время фиксации. Категория события.
9.	Технические системы и средства досмотра. Обнаружитель паров и следов взрывчатых веществ	Обнаружение паров и следовых количеств взрывчатых веществ, превышающих установленные пороговые значения.	Время фиксации. Категория события. Изображение, формируемое досмотровой системой.

ВЫВОДЫ:

1. ***Рекомендуется использование на объектах культуры интегрированной системы, объединяющей сигналы от всех систем жизнеобеспечения в едином программном поле.***
2. ***Интеграция систем позволяет повысить уровень защиты объекта и сократить время реакции на события.***
3. ***Решения по интеграции систем рекомендуется закладывать на стадии проектирования или модернизации систем жизнеобеспечения здания.***

ГЛАВА 5.8. ПРИНЦИПЫ ОРГАНИЗАЦИИ ДИСПЕТЧЕРСКОГО ПУЛЬТА ВИДЕОНАБЛЮДЕНИЯ

Диспетчерский пульт наблюдения является составной частью комплексной системы безопасности и предназначен для централизованной охраны ряда рассредоточенных объектов, приема от оконечных устройств событий, служебных и контрольно-диагностических извещений, влияющих на безопасность контролируемых объектов, обработки, отображения, регистрации полученной информации и представления ее в заданном виде для дальнейшей обработки, а также для передачи на оконечные объектовые устройства команд телеуправления.

Как правило, в диспетчерский пульт поступает информация не только от инженерно-технических средств охраны, но и от различных инженерных систем жизнеобеспечения зданий, автоматизированных систем управления технологическими и производственными процессами, систем служебной связи. При этом через диспетчерский пульт осуществляется управление силами обеспечения безопасности на объектах путем ситуационного реагирования на возникшую угрозу безопасности или реализации автоматических сценариев реагирования, обеспечивающих выполнение заранее заданного порядка действий в соответствии с принятыми для охраняемых объектов стандартами безопасности.

Техническую основу работы диспетчерского пульта управления составляет система сбора и обработки информации, позволяющая принимать данные и передавать команды управления на инженерно-технические средства охраны (ИТСО).

К инженерно-техническим средствам охраны относятся:

1) **инженерно-технические средства защиты:**
   инженерные заграждения; инженерные средства и сооружения: контрольно-пропускные пункты, помещения для размещения подразделений охраны;
2) **технические средства охраны:**
   a) система охранно-тревожной сигнализации;
   b) система охранная телевизионная;
   c) система контроля и управления доступом;
   d) система автоматической пожарной сигнализации и пожаротушения;
   e) система сбора и обработки информации, включающая подсистему связи и передачи извещений к пунктам централизованного наблюдения;
   f) технические средства досмотра.
3) **вспомогательные системы:**
   a) система охранного освещения;
   b) система оповещения о тревоге, чрезвычайной ситуации и др.;
   c) система электропитания;
   d) система оперативной связи подразделений охраны;
   e) иные интернированные подсистемы обеспечения безопасности.

Инженерно-технические средства защиты

Инженерно-технические средства защиты объекта должны обеспечивать круглогодичную защищенность объекта от актов незаконного вмешательства путем разрушения, взлома строительных защитных конструкций, преодоления ограждений, вскрытия запирающих устройств и предназначены для:

a) создания физических преград несанкционированным действиям в отношении объекта;
b) создания препятствий на пути движения нарушителя с целью затруднения (задержки) его продвижения к уязвимым местам, критическим элементам и на пути отхода на время, достаточное для силового или технологического реагирования, с целью минимизации возможного ущерба;
c) обнаружения следов нарушителя, определения направления его движения;
d) обеспечения прохода в охраняемые зоны только в установленных точках (пунктах) доступа;
e) обозначения границ охраняемых зон и предупреждения об ответственности за нарушение права собственности;
f) предотвращения таранного удара (прорыва) транспортными средствами уязвимых мест объекта;
g) защиты обслуживающего персонала и посетителей объекта.

ПРИМЕЧАНИЕ: ***Инженерно-технические средства защиты должны повышать эффективность функционирования системы физической защиты объекта.***

Охранно-тревожная сигнализация

Система охранно-тревожной сигнализации должна обеспечивать получение и обработку тревожных извещений с периметральных средств обнаружения, автоматических и неавтоматических извещателей, возможность учета и хранения сигнальной информации, отображения информации о тревожных событиях.

Система охранно-тревожной сигнализации включает в себя следующие технические средства:

a) периметральные средства обнаружения, предназначенные для обнаружения нарушителей на открытых площадках (периметр объекта, границы локальных зон и др.);
b) средства обнаружения проникновения – автоматические и неавтоматические охранные и тревожные (тревожная сигнализация) извещатели, предназначенные для охраны внутри помещений;
c) средства сбора и обработки информации – приборы приемноконтрольные, а также блоки, устройства и модули в составе комплексных (интегрированных) систем, обеспечивающие прием извещений от охранных извещателей, обработку и отображение информации, осуществление местного звукового и светового оповещения, управление взятием (снятием) и передачу информации о состоянии охраняемого объекта (зоны) на пункт централизованного наблюдения;
d) вспомогательные системы.

Система контроля и управления доступом

Система контроля и управления доступом объекта должна обеспечивать:

a) санкционированный доступ и предотвращение несанкционированного доступа людей и транспорта на объекты, в отдельные зоны, здания и помещения;
b) выдачу информации на пункт диспетчерского наблюдения комплекса инженерно-технических средств охраны о попытках несанкционированных действий в отношении объекта;
c) работоспособность в автономном и сетевом режиме с автоматическим переходом из первого во второй при обрыве связи, нарушении локальной вычислительной сети (универсальность системы).

Технические средства досмотра

Технические средства досмотра применяются для обнаружения оружия, других запрещенных к проносу (провозу) предметов и веществ при проходе людей или въезде транспортных средств на охраняемый объект, а также для предотвращения актов незаконного вмешательства.

Перечень технических средств досмотра включает в себя:

a) металлообнаружители (стационарные, переносимые);
b) досмотровые рентгенотелевизионные комплексы;
c) досмотровые эндоскопы и зеркала;
d) средства радиационного контроля;
e) обнаружители опасных химических и взрывчатых веществ.

Металлообнаружители (металлодетекторы) осуществляют обнаружение металлических объектов поиска холодного и огнестрельного оружия, металлосодержащих взрывчатых устройств, различных видов металлосодержащей продукции, запрещенных к проносу. Они выполняются в виде стационарных устройств арочного типа (порталы) либо в виде портативных переносных приборов.

Рентгенотелевизионные досмотровые комплексы применяются для определения содержимого проносимых и провозимых на территорию объекта предметов и должны обеспечивать обнаружение и пресечение провоза/проноса оружия, взрывчатых, наркотических веществ и запрещенных предметов.

Досмотровые эндоскопы и зеркала применяются для визуального осмотра труднодоступных мест в транспорте, выявления в них взрывчатых устройств, огнестрельного и холодного оружия, других запрещенных к провозу предметов.

Аппаратура для обнаружения взрывчатых и опасных химических веществ применяется для выявления их наличия или следов путем проведения анализа подозрительных проб воздуха. Она должна фиксировать наличие обычных взрывчатых веществ типа тротил, гексоген, пластид и обеспечивать экспресс-выявление следов взрывчатых веществ на поверхности предметов.

Система сбора и обработки информации

Система сбора и обработки информации (ССОИ) предназначена для выполнения следующих основных функций:

a) прием извещений и передачу команд управления в инженерно-технические средства охраны (ИТСО), систему видеонаблюдения и биометрической идентификации, автоматизированные системы управления технологическими процессами и иные автоматизированные системы, участвующие в работе диспетчерского пульта управления;
b) выявление зависимостей в извещениях, полученных от различных систем, оценка возникновения угроз безопасности и формирование инцидентов, требующих обработки оператором;
c) информационно-аналитическое сопровождение операторов диспетчерского пульта;
d) выполнение автоматических сценариев реагирования;
e) формирование карточек инцидентов и долговременное хранение связанных с ней данных, полученных из ИТСО, протоколирование действий операторов системы, создание отчетов;
f) мониторинг персонала.

Подсистема приема-передачи извещений

В части информационного обмена ССОИ должна обеспечивать прием данных от систем охранной и периметровой сигнализации, системы контроля и управления доступом, досмотровой техники, включая уловители взрывчатых веществ, металлодетекторы, интроскопы и прочее оборудование с целью выявления пожара на стадии возгорания, попыток проноса запрещенных предметов на территорию объектов предприятия, попыток нарушения внутриобъектового режима сотрудниками предприятия и посетителями, а также обнаружения несанкционированного проникновения на объекты предприятия.

В части информационного обмена с системами видеонаблюдения и биометрической идентификации ССОИ должна обеспечивать:

a) получение изображений с телевизионных камер системы видеонаблюдения в режиме реального времени и из видеоархива;
b) прием информации о сработках видеоаналитических детекторов, в том числе о саботаже камер, оставленных предметах, скоплении людей, числе посетителей, действиях персонала, контроле ношения средств индивидуальной защиты и соблюдения требований техники безопасности, пересечении линий, обнаружении дыма и огня и прочего;
c) информационный обмен с системой биометрической идентификации в части ведения черного и белого списков, категоризации посетителей, совмещения результатов биометрической идентификации с проходами СКУД.

В части информационного обмена с инженерными системами ССОИ должна обеспечивать прием данных об исправности того или иного оборудования, режимах его функционирования, текущего состояния систем.

ВАЖНО! ***В случае выявления отклонений от нормального функционирования ССОИ должна инициировать формирование карточки инцидента и запускать заранее настроенные сценарии реагирования.***

Информационно-аналитическая подсистема

Информационно-аналитическая подсистема предназначена для информационного обеспечения операторов диспетчерского пульта и выполняет следующие функции:

- контроль за обеспечением безопасности на объектах предприятия;
- оперативная оценка, анализ и прогнозирование обстановки на объектах предприятия;
- отображение информации о состоянии защищенности объектов предприятия на электронной карте;
- снабжение персонала подразделений безопасности информацией, необходимой для повышения антитеррористической защищенности объектов предприятия, а также защиты объектов от пожаров, несанкционированного проникновения людей, краж, вандализма в режиме реального времени;
- оповещение о нападении на сотрудников предприятия, контроль за действиями служб быстрого реагирования;
- контроль за работой персонала на объектах предприятия, предоставление информации о совершенных правонарушениях с указанием времени, места, данных сотрудника, а также предоставление видеофрагмента;
- своевременное и наглядное представление руководству предприятия отчетной, аналитической и прогнозной информации, необходимой для принятия решений, в том числе на мобильных устройствах;
- поддержка процессов принятия управленческих решений по своевременному предупреждению и ликвидации нештатных ситуаций;
- организация взаимодействия по вопросам обеспечения безопасности с информационными системами предприятия.

Автоматические сценарии реагирования

Сценарий реагирования представляет собой алгоритм действий, заданный для определенного типа инцидента, который исполняется в автоматическом режиме при срабатывании определенного правила. Сценарий позволяет в автоматическом режиме выполнять множество действий и распараллеливать операции, тем самым ускоряя процесс реагирования и избавляя операторов диспетчерского пункта от осуществления рутинных действий вручную. Сценарий реагирования может включать в себя как действия, направленные на сбор дополнительной информации, так и необходимые первоочередные шаги для реактивных действий на возникшую угрозу безопасности, а также максимально оперативного уведомления всех заинтересованных сторон в соответствии с зонами ответственности и планирование последующих задач по обработке и аналитике.

Фиксация плана действий по реагированию в виде сценария позволяет снизить человеческий фактор и вероятность ошибки или пропуска какого-либо этапа. Контроль выполнения операций и возможность скорректировать их на лету позволяют гибко управлять процессом реагирования.

Критерии для срабатывания сценариев определяются механизмом обработки поступающих событий из подсистемы приема-передачи извещений. Помимо самих критериев необходимо задать правила их срабатывания, которые могут учитывать различные варианты соответствия (всем критериям, одному из критериев или пользовательской комбинации условий).

В состав сценария могут быть включены следующие типы действий:

- **Сбор информации** – выгрузка дополнительной информации в автоматическом режиме из смежных систем: логи, дампы, состояния систем и пр.
- **Уведомление** – позволяет отправить уведомление выбранным пользователям или группам пользователей. Уведомления могут быть следующих видов:
  - звуковое оповещение операторов;
  - визуальное оповещение (всплывающая нотификация, акцентирование внимания на элементах пользовательского интерфейса, графическая аннотация и пр.);
  - отправка СМС-, e-mail-, telegram-уведомлений произвольного содержания или по ранее заданным шаблонам.
- **Категоризация инцидента** – присвоение категории угроз по совокупности признаков посредством DMN-инструментов.
- **Создание списка объектов** из смежных систем, связанных с возникшим инцидентом.
- **Управление смежными системами**:
  - Запись видео по камерам из списка с таким-то профилем записи;
  - Извлечение видеоархива по камерам из списка;
  - Смена/заполнение раскладок видеостены или пользовательского интерфейса;
  - Управление поворотными и исполнительными устройствами;
  - Управление сервером картографии: позиционирование, фильтры информационных слоев, применение цветовых схем и пр.
- **Запуск скриптов в смежных системах.**
- **Пользовательское задание** – позволяет добавить действие, которое должен совершить пользователь в отношении инцидента, с указанием типа запуска (сразу, после завершения другого действия и т. д.). Например, это может быть получение подтверждения от патруля/наряда о том, что инцидент не произошел по причине ложного срабатывания устройств.
- **Создание отчета** по заранее подготовленному шаблону.
- **Запуск другого сценария** – позволяет запустить сценарий реагирования из списка сценариев, существующих в системе;

ПРИМЕЧАНИЕ: ***Сценарий можно представить как процесс в нотации BPMN/CMNN/DMN с описанными действиями. Представление в такой нотации позволяет превращать аналитические диаграммы в исполняемые модели технологических процессов. Благодаря этому модель процесса реагирования будет отражать реальную последовательность действий, которую необходимо будет выполнить в действительности.***

На **рис. 27** представлен пример процесса в нотации BPMN.

Рис. 27. Пример процесса в нотации BPMN

Мониторинг персонала

Система мониторинга персонала предназначена для обеспечения безопасности сотрудников предприятия и должна обеспечить непрерывный контроль местонахождения персонала и сил безопасности на открытых территориях с функцией обратной связи с диспетчером.

Функциональные возможности:

- непрерывный мониторинг персонала, перемещения и направление перемещений персонала по маршрутам движения;
- передача данных о местоположении персонала по доступным каналам связи;
- визуальное отображение контролируемых зон, в которых на текущий момент зарегистрирован персонал;
- автоматизированный контроль соблюдения сотрудниками маршрута движения;
- формирование технологических отчетов в части мониторинга местоположения и маршрутов перемещения персонала, учет отработанного времени.

Архитектура системы диспетчеризации должна обеспечивать выполнение следующих ключевых требований:

- иерархичность;
- масштабируемость – возможность расширения системы без изменения ее архитектуры. Необходимо учесть возможность модернизации систем безопасности объектов предприятия, а также поэтапный ввод в эксплуатацию отдельных подсистем;
- функциональность – способность централизованно предоставлять заданный набор ИТ-сервисов;
- доступность ресурсов – гарантированное предоставление требуемых ресурсов в нужное время;
- производительность – гарантированное обеспечение функциональности при расчетных нагрузках;
- достоверность данных – гарантии невозможности несанкционированного изменения данных;
- резервирования инфраструктуры – нечувствительность к сбоям и отказоустойчивость на всех уровнях иерархической архитектуры.

Схематично система диспетчеризации представлена на **рис. 28**:

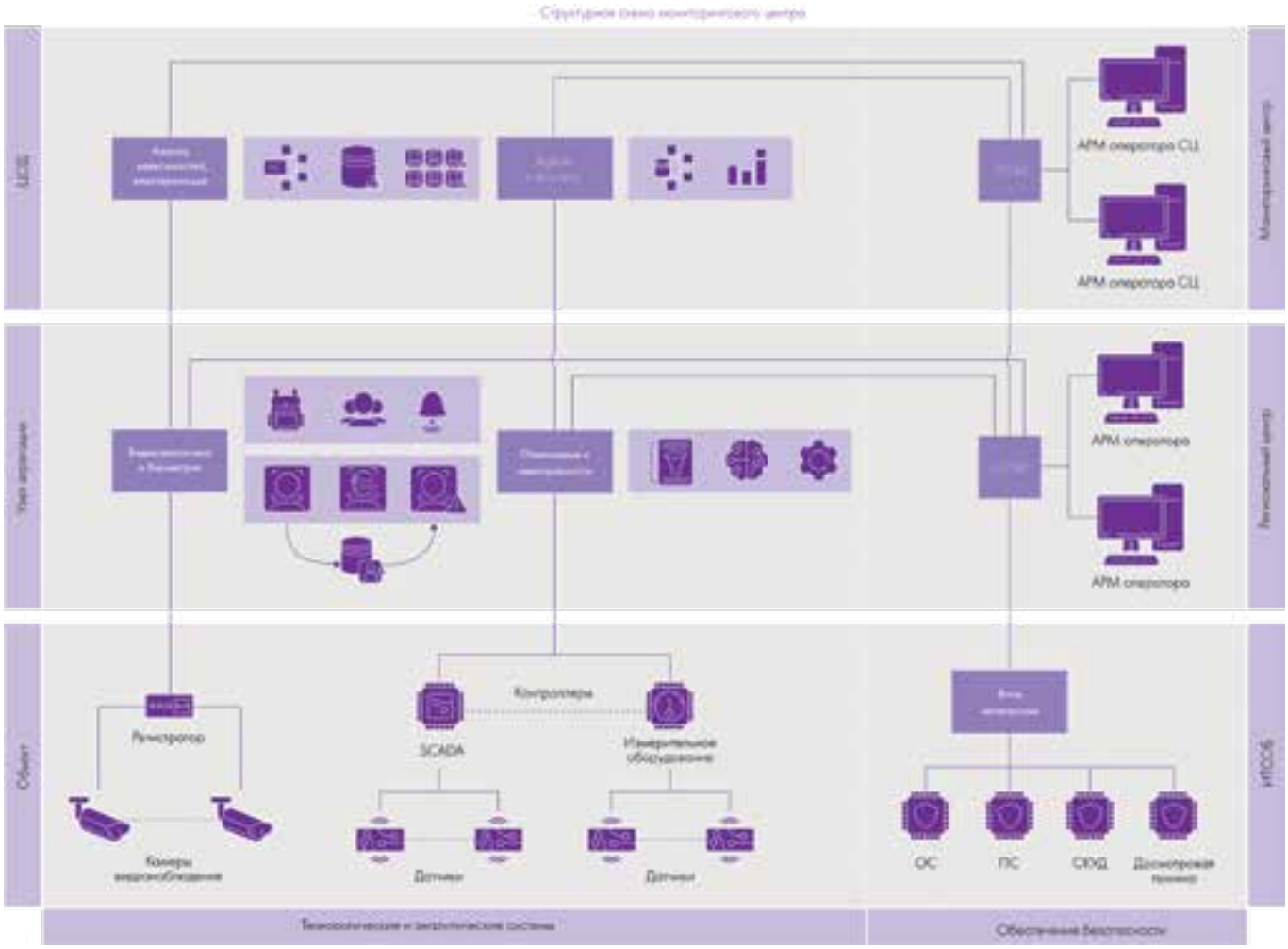


Рисунок 28. Схема системы диспетчеризации

Рабочее место оператора

Рабочее место оператора должно быть приспособлено к психофизическим свойствам человека в зависимости от вида и характера выполняемой работы. При рассмотрении вопросов организации диспетчерского пульта видеонаблюдения следует принимать во внимание механизмы человеческого зрения и общую физиологию восприятия информации. Эффективность работы оператора связана с общим количеством одновременно отображаемых видеокамер, количеством поступающих тревог в единицу времени, а также уровнем автоматизации реакции на события.

На **рис. 29** приведены средние значения углов зрения человека и величина оптимального угла вращения глаза. При выборе количества, типа мониторов и способа организации видеостены следует в первую очередь опираться на данные параметры.

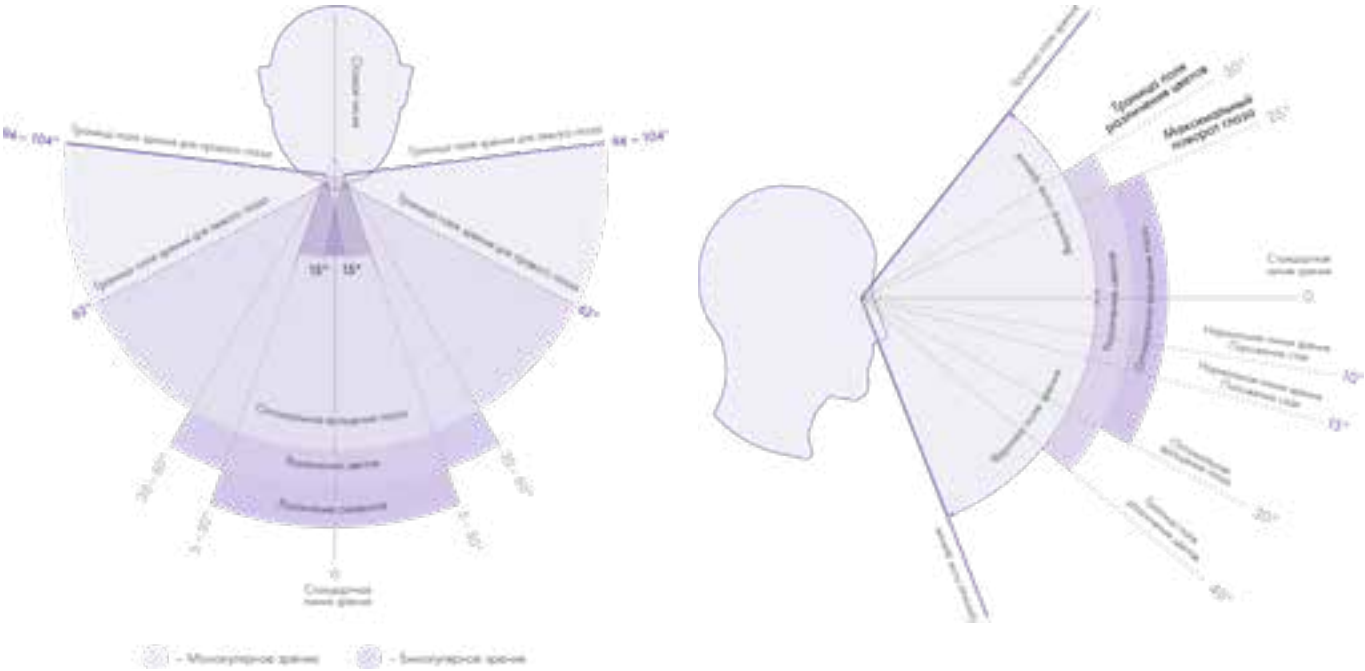


Рис. 29. Значения углов зрения человека

ВАЖНО: ***Оптимальное расстояние по горизонтали от монитора до оператора зависит от диагонали монитора и составляет приблизительно 3–4 диагонали монитора, например, при использовании мониторов диагональю 24 дюйма оптимальное расстояние до оператора составит 1,80–2,40 м.***

Количество мониторов может отличаться в зависимости от совокупности различных факторов (количество видеокамер, площадь объекта, уровень безопасности и т. д.).

Единые требования в области организации системы видеоотображения не установлены нормативной документацией, на практике часто применяется компоновка мониторов с разделением по функциональному назначению:

1. **Тревожные мониторы** – отображение видеокамер и событий, имеющих приоритет над остальными и требующих особого внимания оператора.
2. **Оперативные мониторы** – отображают раскладку изображений, соответствующих текущей задаче оператора (контроль экскурсионных групп, входной зоны, погрузка экспонатов и др.).
3. **Справочные или дежурные мониторы** – отображение видеокамер для общего контроля ситуации на объекте. Размер изображения камеры на мониторе должен быть выбран исходя из условия оценки обстановки контролируемой зоны одним взглядом оператора.

Примерная структура видеостены с использованием указанной компоновки приведена на **рис. 30**.

При использовании нескольких рядов мониторов возможно размещение кронштейнов полукругом (в боковой проекции) для сохранения равных расстояний от места работы оператора.

Количество сигналов тревоги для одного события, которые получает оператор, должно быть минимизировано для снижения нагрузки на оператора. Согласно СанПиН 1.2.3685-21 «плотность сигналов (световых, звуковых) в среднем за час работы» допускается в диапазоне от 76 до 175. Допустимые величины психофизиологических производственных факторов по показателям тяжести и напряженности труда также содержат ограничения по длительности сосредоточенного наблюдения (% от времени смены) – от 26 до 50 – и числу объектов наблюдения – от 6 до 10.

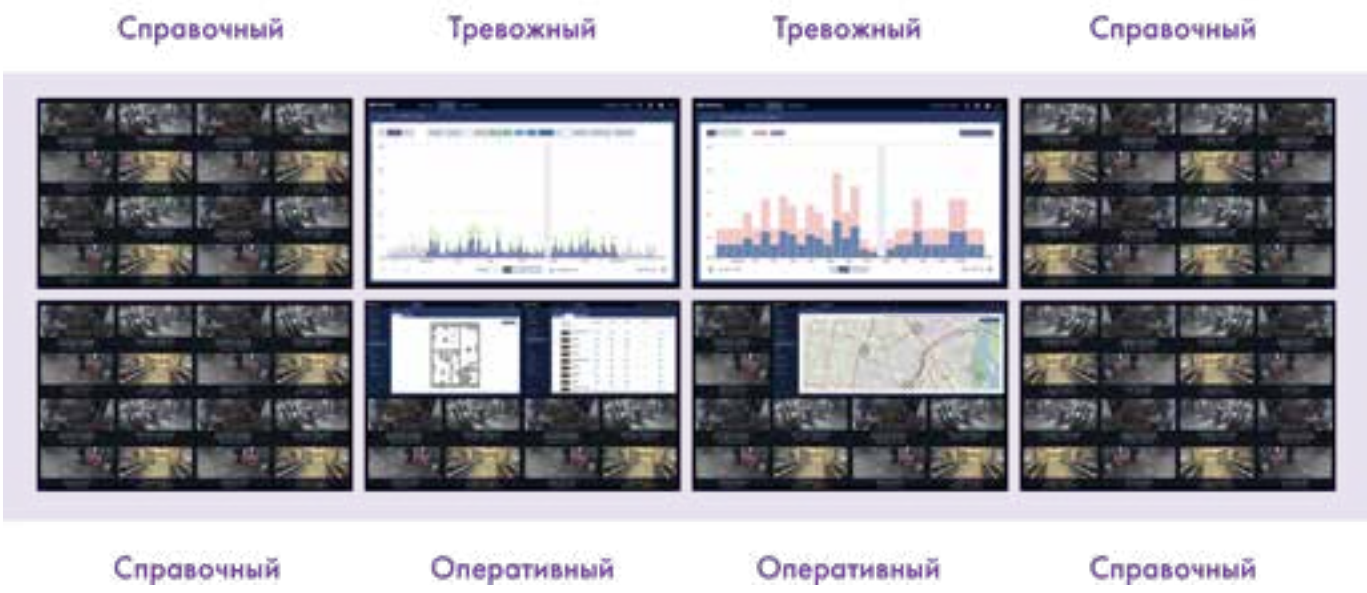


Рис. 30. Пример структуры организации видеостены

ВЫВОДЫ:

1. Важно настроить систему видеонаблюдения таким образом, чтобы в соответствии с возникающей ситуацией в данный момент пользователь мог получить наиболее полную и адаптированную к текущим потребностям информацию.

2. Размещение систем принятия решений в одном месте помогает добиться лучшей организации работы операторов отдельных систем, характеризующейся более быстрым обменом информацией и принятием согласованных решений, связанных с функционированием объекта, а также реагированием на возникающие опасности.

3. Следует уделять особое внимание организации рабочего места оператора с учетом физиологических особенностей человека.

ГЛАВА 5.9. ВИДЕО- И АУДИОАНАЛИТИКА

Выбор типа аналитики зависит от поставленных задач. Принятие решения в пользу ее использования рекомендуется делать после проведенного тестирования. В приоритете аналитика на базе ИИ, работа которой существенно снижает количество ложных срабатываний. Видеоаналитика обращает внимание оператора на нештатные ситуации, что помогает ему вести наблюдение на объекте. Именно поэтому важно правильно выбрать и настроить систему.

5.9.1. ВСТРОЕННАЯ В КАМЕРЫ ВИДЕОАНАЛИТИКА

Обычно на стороне камеры установлена простая видеоаналитика, не требующая много вычислительных ресурсов. Рекомендуется использовать нижеуказанные детекторы на базе нейросети.

К такой аналитике относятся следующие детекторы:

- Праздношатание.
- Пересечение линии.
- Вторжение в зону.
- Саботаж.
- Определение направления движения.
- Детектор отсутствия/наличия медицинской маски.
- Детектор толпы.
- Маскирование лица/тела.
- Распознавание лиц.
- Распознавание номеров.

Рис. 31а. Виды видеоаналитики: вторжение в зону

Рис. 31б. Виды видеоаналитики: неправильное направление

Рис. 31в. Виды видеоаналитики: пересечение линии

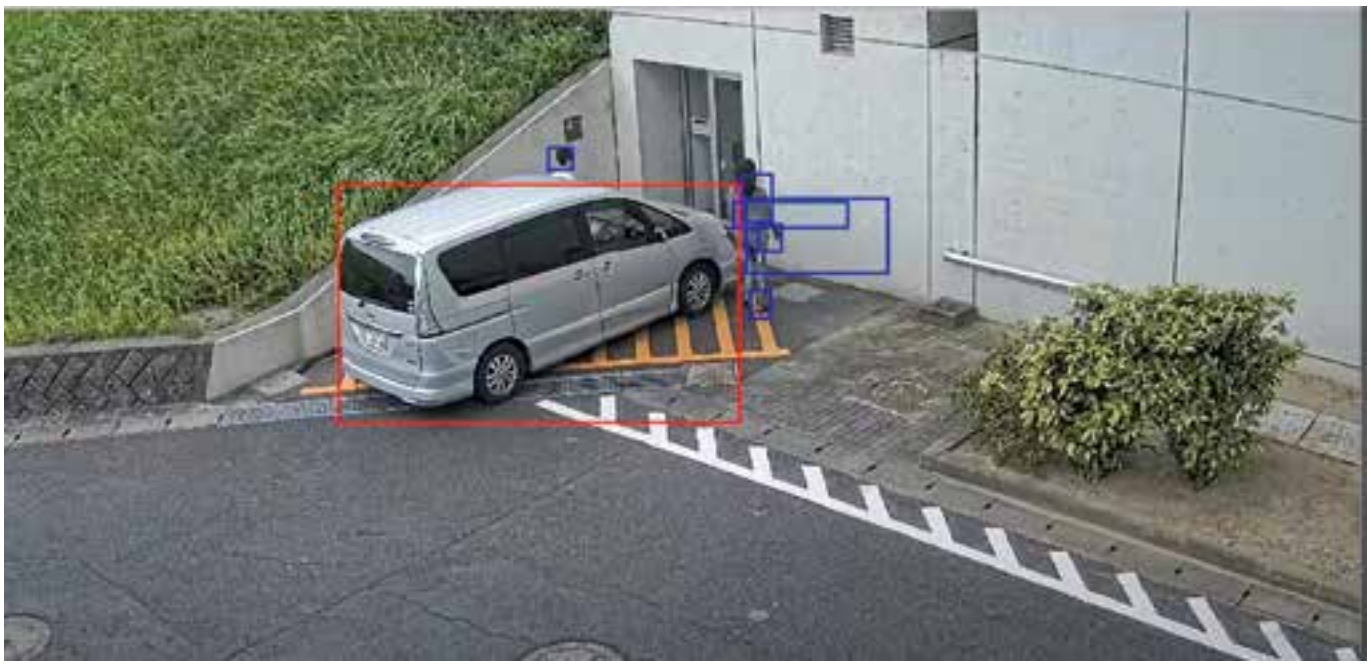


Рис. 31г. Виды видеоаналитики: праздношатание

Рис. 31д.
Виды видеоаналитики: обнаружения изменения сцены/саботаж

ВАЖНО! ***Распознавание лиц и автономеров может происходить на стороне камеры, а сопоставление с базой, поиск в черных и белых списках, а также алгоритм действия производится на стороне сервера аналитики.***

В случае использования встроенной в камеры аналитики необходимо убедиться, что данное оборудование полностью (видео и аналитика) интегрированы в выбранное программное обеспечение.

Рекомендации по применению:

1. Праздношатание (использование у банкоматов для вычисления злоумышленников).
2. Изменение сцены / расфокусировка объектива и пр. (исключение саботажа, применяется в местах наблюдения за важными объектами).
3. Пересечение линии, вторжение в зону и пр. применяется для ограничения доступа к объектам экспозиции, таким как воссозданные элементы быта, картины и др., обеспечение детекции по периметру (используется для снижения нагрузки на оператора, но есть вероятность ложных срабатываний, рекомендуется проводить тестирование).

5.9.2. СЕРВЕРНАЯ ВИДЕОАНАЛИТИКА

Серверная видеоаналитика используется:

- **Если установленные/выбранные камеры не поддерживают вышеупомянутые встроенные детекторы.**

В этом случае камеры будут отправлять видеоданные на сервер аналитики, где будет происходить дальнейшая обработка и анализ изображения.

- **Если нельзя решить поставленные задачи существующими в камерах функциями.**

К таким задачам часто относят специализированную видеоаналитику, которая не реализована на видеокамерах или создана по ТЗ заказчика. Применение распределенной видеоаналитики, когда видеокамера определяет нарушение и отправляет данные (метаданные) на сервер, в значительной мере экономит серверные ресурсы, что позволяет подключить большее количество периферийных устройств.

ПРИМЕЧАНИЕ: ***Определение экономической выгоды от использования той или иной схемы построения системы зависит от многих факторов, например стоимость периферийных устройств и программного обеспечения, качество интеграции, стабильность работы и требования к вычислительным мощностям.***

5.9.3. АУДИОАНАЛИТИКА

Звуковой анализ ситуации, как и видеоаналитика, применяется для оперативного выявления нештатных ситуаций, а именно: разбития стекла, выстрела, крика, срабатывания сигнализации автомобиля, взрыва. Для их детектирования звуки должны быть громкими и/или резкими, что исключает их использование при обнаружении конфликтных ситуаций, когда разговор идет на повышенных тонах, но не превышает критических значений. Данные функции реализованы как на базе видеокамеры, так и на базе сервера. Выбор схемы построения системы зависит от используемого программного обеспечения и поставленных задач.

ГЛАВА 5.10. ОСОБЕННОСТИ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ, ЭКСПЛУАТАЦИИ И ПРОЕКТИРОВАНИЯ

1. Организация серверной

Одной из важнейших составляющих бесперебойной работы системы видеонаблюдения является правильная организация помещения серверной (серверных шкафов при отсутствии отдельного помещения).

Обеспечение комплекса мер по оснащению серверной средствами безопасности и жизнеобеспечения позволяет продлить срок службы оборудования и избежать возникновения возможных угроз, таких как:

- выход из строя центрального оборудования видеонаблюдения в результате инцидентов на объекте (отключение электроэнергии, перегрев, протечка, пожар и др.);
- нарушение режима сохранения конфиденциальности информации;
- случайные вмешательства в работу системы.

Ряд мер по организации телекоммуникационных комнат и серверных помещений определен следующими нормативными документами:

1. ГОСТ Р 58242-2018. Национальный стандарт Российской Федерации. Слаботочные системы. Кабельные системы. Телекоммуникационные пространства и помещения. Общие положения.

2. СП 486.1311500.2020. «Системы противопожарной защиты. Перечень зданий, сооружений, помещений и оборудования, подлежащих защите автоматическими установками пожаротушения

и системами пожарной сигнализации. Требования пожарной безопасности», утвержденный приказом МЧС России от 20 июля 2020 года № 539.

Внутри помещений серверной комнаты (аппаратной) должны быть обеспечены следующие условия:

- микроклимат с показателями температуры 18–24 °С, влажности 30–55 %. В связи с тем что серверные устройства преимущественно затягивают воздух с лицевой стороны, а выбрасывают с тыльной стороны, рекомендуется организовывать охлаждение серверных стоек с физическим разделением на холодный и горячий коридоры для повышения энергоэффективности;
- рекомендуется поддерживать избыточное давление при смене всей массы воздуха в течение одного часа;
- полы, стены и потолки в аппаратных рекомендуется обрабатывать средствами, препятствующими оседанию и накоплению пыли, предельно допустимая концентрация уровня пыли не более 100 мг/м^3;
- электропитание от отдельного электрического щита;
- при площади помещения до 24 м^2 обязательно оснащение системой пожарной сигнализации;
- при площади помещения 24 м^2 и более обязательно оснащение автоматической установкой пожаротушения. Рекомендуется использование газового огнетушащего вещества;
- недопустимо размещение в серверной трубопроводов, дренажных систем, открытого конденсата. Должна быть обеспечена гидроизоляция потолков и система защиты от протечек;
- доступ в помещение серверной должен иметь ограниченный круг лиц, телекоммуникационные шкафы должны быть оборудованы замками и находиться в закрытом состоянии.

2. Особенности эксплуатации систем видеонаблюдения

Использование системы видеонаблюдения возлагает на пользователя определенные эксплуатационные затраты в части технического обслуживания. Основной регламент технического обслуживания приведен в **Приложении**. В данном разделе отмечены особенности эксплуатации систем видеонаблюдения, которые рекомендуется учитывать при проведении ТО или проверке выполнения работ сторонней подрядной организацией.

ВАЖНО! ***Проведение работ по техническому обслуживанию системы видеонаблюдения на объектах культурного наследия или в непосредственной близости от экспонатов, в частности прокладка кабельных линий, установка и регулировка видеокамер должны проводиться только после получения соответствующих согласований при условии обеспечения безопасности для экспонатов и здания.***

Видеокамеры, применяющиеся для мониторинга обстановки внутри зданий и на территории, часто располагаются в местах, где присутствуют риски, связанные с возможным падением человека с высоты. Проведение работ по регулярной очистке таких видеокамер должно производиться в строгом соответствии с действующими Правилами по охране труда при работе на высоте. При проведении технического обслуживания обязательна проверка соответствия требований, указанных в инструкции по эксплуатации оборудования. Нарушения герметичности уличных видеокамер, отсутствие подключения к системе уравнивания потенциалов и другие отклонения от инструкций несут высокие риски выхода из строя оборудования.

ВАЖНО! ***Регулярная проверка качества изображения со всех видеокамер является крайне важным пунктом технического обслуживания, особенно в случае крупных систем, когда оператор не может единовременно наблюдать изображение со всех видеокамер.***

Изменение внешних условий, например установка нового уличного фонаря, может привести к получению неинформативной картинки с видеокамеры в результате полной засветки. В процессе эксплуатации нередко можно столкнуться с расфокусировкой объектива либо перекрытием зоны обзора видеокамеры предметами (шкафами, витринами и т. п.). Следует отметить, что во многих системах видеонаблюдения производителями закладывается функционал обнаружения видеокамерой внешних условий (засветка, затемнение, маскировка и т. п.). При наличии данной функции рекомендуется настройка автоматической отправки тревожного сообщения об изменении условий на диспетчерский пульт. Помимо проверки текущего изображения с видеокамер требуется регулярная проверка записи видеоархива.

ВАЖНО! ***Прерывание записи в случае неисправности обязательно должно сопровождаться отправкой тревожного сообщения оператору для своевременного реагирования.***

3. Особенности проектирования систем видеонаблюдения с использованием технологии информационного моделирования – BIM

15 сентября 2020 года председатель Правительства Российской Федерации Михаил Мишустин подписал **постановление № 1431 «Об утверждении правил формирования и ведения информационной модели объекта капитального строительства, состава сведений, документов и материалов, включаемых в информационную модель объекта капитального строительства и представляемых в форме электронных документов, и требований к форматам указанных электронных документов, а также о**

внесении изменения в пункт 6 Положения о выполнении инженерных изысканий для подготовки проектной документации, строительства, реконструкции объектов капитального строительства».

Постановление вводит в России новый градостроительный подход с использованием информационной модели – Building Information Model (BIM). Применение этой технологии позволяет отслеживать состояние объекта на протяжении всего жизненного цикла, способствует улучшению качества строительства, снижает риски серьезных ошибок и потерь при реализации масштабных проектов.

BIM – это инновационный подход, как к строительству зданий, так и к обеспечению его безопасности. Кроме того, современные технологии информационного моделирования открывают новые возможности в оценке эффективности управления эксплуатацией объекта. BIM позволяет делать более точные экономические расчеты. Так, например, проект системы видеонаблюдения состоит из многих элементов, включающих конкретные технические средства, оборудование (в том числе видеокамеры и т. п.), у которых есть свои технические и стоимостные характеристики. Четкая и стройная методология BIM позволяет просчитать, сколько нужно ресурсов, в том числе финансовых, чтобы его смонтировать на конкретной площадке.

Ключевые нюансы BIM-проектирования системы видеонаблюдения:

а) Наглядная визуализация
Одно из ключевых преимуществ в том, что современные модули BIM-проектирования позволяют в автоматическом режиме создать 3D-вид, который будет имитировать то, что в реальности увидит диспетчер на мониторе видеонаблюдения. Созданный вид учитывает углы обзора (в том числе для вариофокальных объективов), угол поворота, наклона и прочие параметры, влияющее на итоговое изображение. Заказчик получает визуальную раскладку всего проекта в максимальной детализации с техническими характеристиками.

б) Детализация
Уровни детализации и наполненности таковы, что максимально исключают возможность ошибок при проектировании систем видеонаблюдения.

в) Контроль изменений в проекте
Проект легко поправить даже на стадии строительства, так, чтобы он соответствовал текущим работам. С помощью BIMDATA можно обнаружить и устранить коллизии на любых, даже самых ранних этапах работы.

г) Технологическое преимущество
Цифровые модели приводят к экономии бюджета проекта до 25 %.

д) Оперативное решение вопросов
Экономия времени на обсуждение и согласование проекта, внесение доработок и принятие решений.

е) Интеграция
На базе BIMDATA создается цифровой скелет здания (объекта), с которым интегрируются проекты всех систем безопасности, в том числе видеонаблюдения. Также копятся данные о выполненной работе, времени, ответственных сотрудниках и службах, поставщиках и т. п.

ж) Экспертиза
Подготовленные цифровые модели могут быть использованы для прохождения государственной экспертизы, так как создаются по всем стандартам Градостроительного кодекса РФ.

6

РАЗДЕЛ Оценка технологических ресурсов систем видеонаблюдения

ГЛАВА

6.1. ОЦЕНКА И ВЫБОР МЕТОДА РЕЗЕРВИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ

Высокая доступность

Высокая доступность – это характеристика системы, которая обеспечивает заданный, обычно превосходящий нормальные значения, уровень производительности и функциональности. Чаще всего высокая доступность выражается во времени беспрерывного доступа к сервисам системы.

Высокая доступность системы достигается за счет правильного выбора архитектуры системы, а также использования специальных механизмов для:

- устранения единой точки отказа отдельных функциональных узлов системы за счет внесения избыточности в защищаемые компоненты системы;
- выявления отказов отдельных узлов и компонентов;
- отказоустойчивого переключения ресурсов для вышедшего из строя узла или компонента системы.

Доступность обычно имеет процентное выражение, при этом принято говорить о числе ***девяток*** для характеристики надежности системы. Так, ***три девятки*** имеет система, сервисы которой работают 99,9 % времени, что эквивалентно тому, что в течение года система находится в неработоспособном состоянии не более 8,77 часа. Для критически важных систем считается нормальной доступность сервисов на уровне 99,995–99,999%, что соответствует 26 и 5,5 минуты отсутствия сервисов в год.

Обеспечение высокой доступности неразрывно связано со способностью системы продолжать работать в случае возникновения сбоев в отдельных ее узлах и компонентах. Такая способность получила название отказоустойчивость.

Обеспечение отказоустойчивости

Отказоустойчивость достигается за счет внесения избыточности в систему, когда создаются дополнительные копии тех или иных элементов системы. В зависимости от назначения этих элементов может применяться один из двух подходов к обеспечению отказоустойчивости:

- дублирование – создание нескольких копий элементов системы, функционирующих параллельно друг другу, при этом результат параллельной работы определяется посредством механизмов нахождения кворума;
- резерв – создание нескольких копий элементов системы и переключение задач на один из свободных элементов в случае сбоя какой-то копии из числа работающих.

Использование механизмов дублирования в вычислительных системах сопряжено с поддержанием консистентного состояния работающих параллельно копий, что гораздо сложнее механизмов резервирования, поэтому данный подход чаще используется для обеспечения отказоустойчивости элементов управления системой.

Для механизмов резервирования принято различать обеспечиваемую степень отказоустойчивости через соотношение активных и резервных элементов. Обычно говорят, что используется N:M резервирование, если для N активных элементов предусмотрено M резервных, на которое производится переключение в случае выхода из строя любого из N активных узлов.

Если для системы используются какие-либо из механизмов обеспечения отказоустойчивости, то принято говорить о кластерном решении, при этом сам по себе кластер – это группа всех, основных и резервных, компонентов системы.

Системы видеонаблюдения в кластере

При необходимости построения масштабируемой и отказоустойчивой системы видеонаблюдения ее компоненты разворачиваются в кластере, состоящим из нескольких физических серверов (либо виртуальных машин), функционирующих под управлением ОС. При этом прикладное программное обеспечение может запускаться в виде контейнеров или в составе образа виртуальной машины под управлением системы оркестрации.

В случае когда компоненты системы видеонаблюдения разворачиваются в виде Docker-контейнеров, централизованное управление их работой обеспечивается системой оркестрации Kubernetes или Docker Swarm. Если же система видеонаблюдения запускается в виде приложения/службы в составе виртуальных машин, то в качестве средства управления могут использоваться платформы OpenStack, Proxmox, VMware и др.

Типовая диаграмма развертывания компонентов системы в кластере показана на **рис. 32**. В построенной по такой схеме системе отсутствует единая точка отказа: все компоненты зарезервированы, выключение любого из узлов кластера приводит к автоматическому перераспределению нагрузки между функционирующими узлами.

В наиболее общем случае можно рассматривать следующие функциональные компоненты системы видеонаблюдения:

- сервер управления в составе узла координации;
- модули ретрансляции в составе узлов доступа;
- модули записи/воспроизведения видеопотоков в составе узлов архива;
- клиентские приложения системы видеонаблюдения;
- СХД – система хранения данных с файловым или объектовым доступом, развернутая в отказоустойчивой конфигурации.

Такое разбиение по функциональному назначению позволяет, во-первых, точнее рассчитывать нагрузку на отдельные компоненты системы в зависимости от ее конфигурации, а во-вторых, гибко масштабировать

систему в зависимости от роста числа одновременных клиентских сессий, камер или емкости архива.

Типы узлов в кластере

Узел координации – хранит конфигурацию системы и осуществляет управление функционированием ее компонентов. Узлы координации ведут мониторинг работоспособности других узлов системы и выполняют перераспределение нагрузки в случае необходимости. На узлах координации функционируют контейнеры с соответствующими службами, а также иные программные компоненты: СУБД, инфраструктурное ПО контейнеризации/виртуализации, балансировщики нагрузки, кластерные средства синхронизации и прочее.

Узел доступа – обеспечивает взаимодействие кластера с внешней сетью (в частности, с интернетом). Запросы, поступающие с клиентских приложений, перенаправляются узлами доступа активным сервисам узлов координации. Кроме того, узлы доступа обеспечивают прием видеопотоков из внешней сети и их ретрансляцию как во внутренние службы кластера (например, для записи в архив), так и внешним потребителям (на рабочие места пользователей). Основными компонентами на узлах координации является один или несколько контейнеров/виртуальных машин с модулями ретрансляции.

Узел архива – производит запись видеопотоков, принимаемых с камер через узлы доступа (сохранение их в виде файлов на СХД). Кроме того, узлы архива отвечают за воспроизведение видеопотоков из архива, получение снимков и экспорт архива (чтение файлов с СХД). На каждом из узлов видеоархива функционирует один или несколько контейнеров с модулем записи/воспроизведения.

Реагирование системы на отказ узлов координации

Узлы координации взаимодействуют между собой на основе алгоритма распределенного консенсуса. Применение этого алгоритма гарантирует консистентность внутреннего состояния системы даже в случае отказа одного из узлов. В основе функционирования алгоритма лежит понятие кворума: решения принимаются только в том случае, если за них проголосовало большинство из узлов кластера. Принятие решений большинством голосов защищает систему от возникновения проблемы split-brain, характерной для распределенных систем.

ВАЖНО! ***Использование кворума накладывает ограничение на минимальное количество узлов координации в системе. Механика кворума не может функционировать, если в системе менее трех узлов координации. При наличии трех узлов отказ одного из них не приводит к сбою: два функционирующих узла координации по-прежнему смогут принимать решения об управлении кластером без учета голоса отказавшего узла.***

При использовании виртуализации виртуальные машины с узлами координации располагаются на разных физических серверах в целях предотвращения их одновременного отключения из-за сбоя оборудования. По этой причине развертывание системы видеонаблюдения в отказоустойчивой конфигурации имеет практический смысл при наличии не менее трех физических серверов. Файлы данных СУБД хранятся на общем блочном устройстве и доступны всем узлам координации, за счет этого отказ узла не приводит к потере доступа к данным.

Реагирование системы на отказ узлов архива

При отказе узлов архива система оркестрации перераспределяет функционировавшие на этом узле контейнеры с модулем записи и воспроизведения между другими физическими серверами или виртуальными машинами с ролью узла архива. Эти контейнеры не хранят персистентного состояния, за счет этого на узлах архива принципиально отсутствует информация, потеря которой является критичной в случае выхода этих узлов из строя: система продолжит функционировать, пока оставшиеся в работе узлы архива имеют достаточно аппаратных ресурсов для обработки заданного набора видеопотоков с камер.

При этом на время переключения записи с вышедшего из строя узла на новую физическую или виртуальную машину данные с видеокамер, привязанных к неисправному узлу, будут потеряны. Для критически важных камер, сохранность данных с которых должна быть устойчива к такого рода отказам, несколько узлов должны принимать их видеопотоки и работать в режиме «горячего» резерва. Другой способ обеспечения непрерывности записи – ведение кратковременного видеоархива на стороне камеры или промежуточных узлов (edge storage) с возможностью синхронизации данных с центральными узлами архивации.

Реагирование системы на отказ улов доступа

Система может включать в себя несколько узлов доступа, и в этом случае пользователи из внешней сети могут работать с ней через любой из них: каждый из узлов доступа имеет свое подключение к внешней сети, а также способен ретранслировать пользователю видеопотоки со всех камер с учетом прав доступа этого пользователя. При отказе узлов доступа система оркестрации перераспределяет функционировавшие на этом узле контейнеры/виртуальные машины с модулем ретрансляции между другими узлами доступа. Как и контейнеры модулей записи/воспроизведения, контейнеры модулей ретрансляции не хранят персистентного состояния и не нуждаются в восстановлении информации при выходе узлов доступа из строя.

В зависимости от программно-аппаратного окружения, в котором разворачивается система, переключение пользователей между узлами доступа в случае их отказа может осуществляться одним из способов:

- средствами внешнего по отношению к системе балансировщика нагрузки (программные или аппаратные балансировщики соединений, а также BGP-маршрутизаторы с поддержкой equal-cost multi-path routing и consistent hashing);
- с использованием технологии плавающих IP, при которой IP-адрес мигрирует между узлами в случае выхода их из строя;
- средствами системы DNS (Round robin DNS, при котором для одного домена задается сразу несколько IP-адресов).

Узлы доступа также обеспечивают поступление видеопотоков с камер в систему видеонаблюдения таким образом, что в любой момент времени к каждому из потоков камер существует не более одного подключения. Общий набор камер распределяется между узлами доступа с использованием алгоритма Rendezvous hashing, и в случае выхода узлов из строя камеры перераспределяются между оставшимися узлами.

Реагирование системы на отказ СХД

При разворачивании системы видеонаблюдения в отказоустойчивой конфигурации необходимо использовать СХД, обладающие встроенными функциями резервирования и отказоустойчивости. Такие механизмы зависят от архитектуры используемой системы, типа предоставляемого доступа (файловый, объектовый, блочный), производителя СХД. В том случае если отказ СХД все же произошел, система видеонаблюдения теряет возможность работы с видеоархивом (в том числе его запись и воспроизведение) до момента восстановления функционирования СХД. Просмотр видео с камер в реальном времени не будет нарушен при отказе СХД.

Масштабируемость системы

Масштабирование системы при увеличении количества обслуживаемых камер или клиентских сессий осуществляется путем добавления в нее новых узлов.

Добавление узлов архива

Необходимое количество узлов архива выбирается исходя из общего количества камер, а также исходя из существующих требований к отказоустойчивости системы. Количество узлов архива, сохраняющих работоспособность при наихудшем из сценариев отказа, должно быть достаточно для того, чтобы обслуживать видеоархив со всех камер системы.

Количество видеопотоков с камер, которое способен обслуживать один узел архива, определяется по некой зависимости от производительности центрального процессора сервера, установленной оперативной памяти, среднего битрейта камеры, а также используемого алгоритма сжатия M-JPEG/H.265/H.265 или др. Точный вид этой зависимости определяется компанией – производителем программного обеспечения для систем видеонаблюдения. Как правило, сам разработчик ПО или проектная организация, хорошо знакомая с продуктами разработчика, имеет в своем распоряжении параметры масштабирования и рекомендации по выбору оборудования.

ВАЖНО! ***Если узлы архива имеют различные аппаратные характеристики (используются различные процессоры либо отличается объем памяти) расчет необходимо вести по наиболее слабому узлу (рекомендуется использовать узлы с одинаковыми характеристиками).***

Добавление узлов координации

Необходимое количество узлов координации определяется требованиями к отказоустойчивости системы. Это количество должно быть таким, чтобы при наихудшем из сценариев отказа, того числа узлов координации, которые остались функционировать, было достаточно для образования кворума узлов, например: при трех узлах координации допустим отказ одного из них (оставшиеся два узла сохраняют кворум), при пяти узлах координации допустим одновременный отказ двух из них (оставшиеся три узла сохраняют кворум).

ВАЖНО! ***Количество узлов координации рекомендуется выбирать нечетное, так как при четном количестве не достигается увеличение уровня отказоустойчивости, например: при четырех узлах координации допустим отказ лишь одного из них, так как отказ двух узлов разрушит кворум.***

Добавление СХД

Хорошим тоном для распределенных систем видеонаблюдения является поддержка нескольких СХД одновременно. Дисковое пространство всех подключенных к системе СХД в таком случае образует единое логическое хранилище видеоархива, в котором нагрузка автоматически распределяется между ними. Производительность СХД в операциях ввод-вывод рекомендуется выбирать не меньше утроенного битрейта всех камер.

Следует также учесть, что, в зависимости от архитектуры системы хранения и компании-производителя, соотношение полезной нагрузки к сырой емкости системы хранения может сильно варьироваться.

ВАЖНО! ***Настоятельно рекомендуется при создании распределенных высоконагруженных систем видеонаблюдения с отказоустойчивыми СХД обращаться к производителю СХД для подбора конфигурации оборудования, расчета необходимых параметров, а также рекомендаций по настройке системы хранения.***

ПРИМЕР КОНФИГУРАЦИИ СИСТЕМЫ

Приведем пример расчета типовой конфигурации распределенной системы, исходя из имеющегося серверного оборудования, проектного количества камер и заданного уровня надежности системы.

Предположим, что мы хотим создать систему, обслуживающую 3000 камер со следующими характеристиками:

- Кодек: H264
- Разрешение: Full HD
- Частота кадров: 25 кадров/с
- Битрейт: 6 Мбит/с

При этом в распоряжении имеются свободные серверы в типовой конфигурации:

- Процессоры: Intel Xeon Silver 4210 (2 шт.)
- Оперативная память: 64 Гбайт
- SSD: 480 Гбайт (2 шт., SAS, RAID 1)

Требования по отказоустойчивости системы:

- Допустим отказ одного узла координации
- Допустим отказ двух узлов архива
- Допустим отказ одного узла ретрансляции

Согласно рекомендациям производителя программного обеспечения установили, что такой сервер позволит обрабатывать до 300 потоков с видеокамер, если его использовать в роли узла архивации, и до 800 потоков в роли узла ретрансляции. В этом случае потребное число таких серверов составит:

- Количество узлов координации: 3
- Количество узлов архива: 12 (10 +2 резерв)
- Количество узлов ретрансляции: 5 (4 +1 резерв)

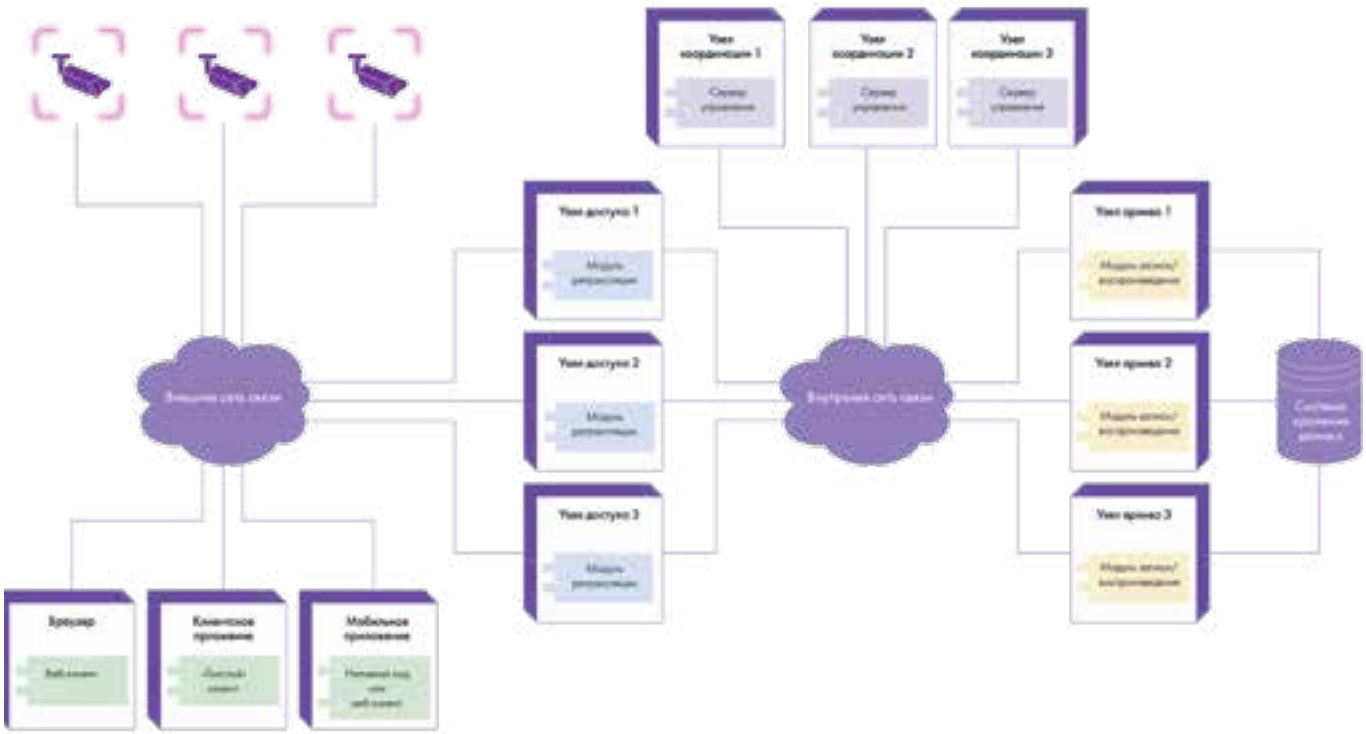


Рис. 32. Типовая диаграмма развертывания компонентов системы в кластере

ГЛАВА 6.2. ОСНОВЫ РАСЧЕТА ПАРАМЕТРОВ СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ ДЛЯ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

Правильный выбор системы хранения данных (СХД) для видеоархива включает в себя определение необходимого полезного объема накопителей, обеспечение требуемой производительности каждого накопителя (или суммарной производительности накопителей при их объединении в массив определенного типа), выбора типа дискового массива, количества избыточных накопителей и накопителей горячего резерва.

Полезный объема СХД определяется суммарным битрейтом (объемом данных в единицу времени, Мбит/с) со всех камер системы. Битрейт каждой камеры зависит от многих факторов: используемого стандарта сжатия, места установки камеры, освещенности области охвата камеры, конструктивных особенностей камеры, особенностей и настроек конкретного ПО для работы с видеопотоком и др. Таким образом, дать точную количественную оценку суммарного битрейта возможно только с поддержкой специалистов заводов-изготовителей и организаций-разработчиков ПО для конкретного выбранного решения. В настоящих рекомендациях приведена методика общей приблизительной оценки требуемого объема СХД. Для получения расчетного

значения полезного объема воспользуйтесь следующей формулой:

V = br × n × d × 10,55

V – необходимый полезный объем СХД в гигабайтах (GB);
Br – расчетный битрейт одной камеры видеонаблюдения в мегабитах при 25 кадрах в секунду (для 2-мегапиксельной камеры со стандартом сжатия H.264 при нормальных условиях эта величина составляет ~3–4 Мбит/с; со стандартом H.265 ~1–2 Мбит/с);
N – расчетное количество камер, подключаемых к СХД;
D – требуемая глубина архива в сутках;
10,55 – коэффициент перевода размерностей.

Пример расчета полезного объема СХД

Исходные данные:

На объекте планируется установить 134 внутренние 2-мегапиксельные камеры видеонаблюдения и 22 дополнительные 4-мегапиксельные уличные видеокамеры для контроля прилегающих территорий и периметра, а также задействовать 19 имеющихся уличных камер (1,3 Мпикс, H.264) для формирования единого видеоархива. Глубина архива – 30 суток.

Для расчета объема СХД необходимо воспользоваться предложенной формулой для каждого типа используемых камер, после чего сложить полученные необходимые объемы хранения. При выборе новых видеокамер целесообразно отдать предпочтение стандарту сжатия H.265, получив расчетные значения битрейта 1,5 и 2 Мбит/с для 2- и 4-мегапиксельных видеокамер соответственно. Битрейт имеющихся камер будет составлять около 3 Мбит/с. Таким образом, получаем следующие выражения:

V1 = 1,5 × 134 × 30 × 10,55 = 63 616,5 ГБ (62,13 ТБ)
V2 = 2 × 22 × 30 × 10,55 = 13 926 ГБ (13,6 ТБ)
V3 = 3 × 19 × 30 × 10,55 = 18 040,5 ГБ (17,62 ТБ)
Тогда общий необходимый полезный объем системы хранения данных будет равен:
$\sum$v = 95 583 ГБайта (93,34 ТБайта)

Полученную величину следует использовать только в целях первичной оценки, так как итоговый объем может быть оптимизирован средствами ПО системы видеонаблюдения, а также должен иметь запас ~25–30 % от минимально необходимого по расчету.

Обеспечение требуемой производительности СХД

Самостоятельная оценка необходимой производительности дисковой подсистемы – задача практически нереализуемая. Наибольшее влияние на итоговое быстродействие окажут алгоритмы записи конкретного программного обеспечения, выбранного для системы видеонаблюдения, используемый стандарт сжатия, количество записываемых кадров в секунду, а также используемый тип дискового массива и особенности работы RAID-контроллера.

Так, при использовании массивов с контролем четности (например, RAID 5 и RAID 6) из-за особенностей алгоритмов записи общая производительность массива может быть ниже производительности одиночного жесткого диска. В общем случае для первичной оценки можно руководствоваться ориентировочной скоростью записи ~80–120 Мбит/с (640–960 Мбит/с) в зависимости от класса предполагаемых для использования жестких дисков. Также нужно учитывать снижение производительности накопителей при одновременном чтении сохраненных данных из архива и в условиях отказа одного (нескольких) накопителей в массиве. С учетом 30-процентного запаса производительности один самостоятельный накопитель или массив типа RAID 5, 6 способен обеспечить скорость записи, соответствующую ~110–160 камерам стандарта сжатия H.264 и 300–450 камерам с кодеком H.265.

Использование дисковых массивов типа RAID 10 обеспечивает несколько бóльшую производительность при записи данных, и такой массив более надежен, но полезный объем для хранения будет составлять только половину от общего объема накопителей в массиве (для RAID 5 полезный объем определяется суммой объемов накопителей в массиве за вычетом одного, а для RAID 6 суммой за вычетом двух).

Расчет необходимого числа накопителей СХД

Произведем ориентировочный расчет необходимого числа накопителей для системы видеонаблюдения из прошлого примера. Наберем необходимую емкость с использованием накопителей номинальным объемом 12 ТБайт. Нужно отметить, что действительный объем любого накопителя будет меньше номинального, так как при производстве считают 1 ТБайт = 10004 Байт (в действительности 1 ТБайт = 10244 Байта), и накопитель номинальным объемом 12 ТБайт будет определен системой как ~10,9 ТБайта.

В прошлом примере необходимый объем хранения составил 93,34 ТБайта, что с учетом 25-процентного запаса составляет 116,68 ТБайта. Для обеспечения такой емкости без формирования какого-либо массива потребуется 11 накопителей:

116 681,9 = 10,7 (11 шт.)

С учетом необходимой избыточности при использовании RAID 5 и RAID 6 потребуется 12 и 13 накопителей соответственно. Для построения RAID 10 в таком случае потребуется 22 жестких диска. **Вне зависимости от типа используемого массива очень важно иметь в СХД 2–3 накопителя горячей замены для своевременного восстановления массива в случае выхода из строя жестких дисков.** Итоговое количество накопителей для разных массивов приведено в таблице:

Тип RAID-массива	Общее количество накопителей (с учетом трех резервных)	Устойчивость к отказу накопителей (количество жестких дисков, выход которых напрямую не влечет потерю данных)		Доля используемого объема хранения (отношение 11 необходимых накопителей к общему числу накопителей в СХД)
Без массива	14	0		0,79
RAID 5	15	1 любой		0,73
RAID 6	16	2 любых		0,69
RAID 10	25	1 любой* *дальнейшие отказы накопителей вызовут потерю данных с вероятностью:		0,44
		1 – 4,76 % 2 – 14,29 % 3 – 27,82 % 4 – 43,86 % 5 – 60,37 %	6 – 75,23 % 7 – 86,79 % 8 – 94,34 % 9 – 98,26 % 10 – 99,37 %	

Пользоваться приведенными данными следует исключительно для формирования концепции или на стадии предпроектных проработок задач организации систем видеонаблюдения. При выборе конкретных технических решений по организации систем хранения видеоархива необходимо всегда руководствоваться рекомендациями производителя выбранного оборудования и программного обеспечения.

ПРИЛОЖЕНИЕ

Типовой регламент технического обслуживания. Минимальный обязательный перечень ежемесячных и ежеквартальных мероприятий по техническому обслуживанию СОТ

Минимальный обязательный перечень ежемесячных мероприятий по техническому обслуживанию (ТО-1) и ежеквартальных мероприятий по техническому обслуживанию (ТО-2) включает в себя перечень работ, указанных в таблице ниже.

Мероприятия по ТО-1 проводятся один раз в месяц в соответствии с согласованным планом-графиком работ по техническому обслуживанию, за исключением месяца проведения ТО-2, в течение всего года, что составляет 8 (восемь) раз.

Мероприятия по ТО-2 проводятся один раз в последнем месяце каждого квартала, что составляет 4 (четыре) раза в течение всего года.

Минимальный обязательный перечень ежемесячных мероприятий по ТО-1 отмечен символом «+» в столбце «ТО-1» в соответствующих строчках таблицы. Выполнение мероприятий в оставшихся строчках не требуется в рамках ТО-1.

Минимальный обязательный перечень ежеквартальных мероприятий по ТО-2 отмечен символом «+» в столбце «ТО-2» в соответствующих строчках таблицы.

№	Содержание работ	Вид работ	
		ТО-1	ТО-2
1.	Внешний осмотр на отсутствие механических повреждений, коррозии; проверка прочности креплений составных частей системы.	+	+
2.	Удаление грязи, пыли, влаги, снега, посторонних предметов с элементов системы. Проверка наличия посторонних шумов, вибрации вентиляторов системы охлаждения видеорегистраторов. Проверка индикации устройств.	+	+
3.	Проверка перехода видеокамер на ночной/дневной режим работы. Проверка корректности функционирования системы видеонаблюдения на предмет неработающих камер, дефектов передачи изображения (яркость, четкость, контрастность, наличие шумов), нерасчетной направленности видеокамер.	+	+
4.	Проверка ведения записи системой видеонаблюдения, настроек записи и глубины архива.	+	+
5.	Корректировка времени на видеорегистраторах.	+	+
6.	Проверка состояния жестких дисков видеорегистраторов по технологии S.M.A.R.T. с формированием отчета для каждого накопителя.		+
7.	Проверка автоматического переключения питания с основного источника на резервный и обратно (для стоечных и компьютерных ИБП). Проверка работы на резервном питании не менее 30 минут.	+	+
8.	Замер емкостей аккумуляторных батарей (для ИБП аналоговых камер видеонаблюдения) с записью показаний для каждой АКБ в соответствующий журнал.	+	+
9.	Проверка автоматического переключения питания с основного источника на резервный и обратно (для ИБП аналоговых камер видеонаблюдения). Проверка работы на резервном питании не менее 30 минут.		+
10.	Проверка корректности работы видеоаналитики.	+	+
11.	Проверка состояния уплотнений и прокладок кожухов камер видеонаблюдения, смена силикагелевого абсорбента и уплотнителей, не обеспечивающих герметичность кожухов.		+
12.	Контроль состояния разъемов и других контактных соединений, обеспечение надежной гальванической связи в контактных соединениях системы.		+
13.	Контроль наличия и корректности маркировок на элементах системы (в том числе кабельных линиях). Восстановление маркировки в случае ее отсутствия или некорректности.	+	+
14.	Проверка соответствия заданных потоков данных сетевых видеокамер. Проверка общей загруженности сетевых коммутаторов.		+

ДОПЕЧАТНАЯ ПОДГОТОВКА

АССОЦИАЦИЯ “БЕЗОПАСНОСТЬ ТУРИЗМА”
115035, г. Москва, Садовническая набережная, д. 7
Тел.: + 7 (495) 151-82-53 (многоканальный)
e-mail: info@tourismsafety.ru
www.tourismsafety.ru