Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерного проектирования

Кафедра проектирования информационно-компьютерных систем

# ПРОЕКТИРОВАНИЕ ЭЛЕКТРОННЫХ СИСТЕМ БЕЗОПАСНОСТИ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

В двух частях

Часть 2

## БЕЗОПАСНОСТЬ В МЕСТАХ МАССОВОГО ПРЕБЫВАНИЯ ЛЮДЕЙ

*Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве пособия для специальности 1-39 02 01 «Моделирование и компьютерное проектирование радиоэлектронных средств»*

Минск БГУИР 2019

УДК [004.056.5+654.9](076.5)
ББК 32.973.202я73+38.48я73
П79

А в т о р ы:
В. В. Хорошко, Д. В. Лихачевский, И. Н. Цырельчук,
В. А. Перевощиков

Р е ц е н з е н т ы:
кафедра автоматизированных систем управления производством
учреждения образования
«Белорусский государственный аграрный технический университет»
(протокол №7 от 04.01.2018);

директор ООО «Авангардспецмонтажплюс»
кандидат технических наук, доцент В. В. Мельничук



П79 **Проектирование** электронных систем безопасности. Лабораторный практикум. В 2 ч. Ч. 2 : Безопасность в местах массового пребывания людей : пособие / В. В. Хорошко [и др.]. – Минск : БГУИР, 2019. – 124 с. : ил.

ISBN 978-985-543-441-3 (ч. 2).

Приведены принципы проектирования интегрированных систем безопасности на примере лицензированного в Республике Беларусь оборудования. Приведены основные требования к проектированию интегрированных систем, предъявляемые действующими на момент написания и издания пособия ТНПА.

Часть 1-я издана в БГУИР в 2017 г.

**УДК [004.056.5+654.9](076.5)**
**ББК 32.973.202я73+38.48я73**

**ISBN 978-985-543-441-3 (ч. 2)**
**ISBN 978-985-543-224-2**

**СОДЕРЖАНИЕ**

## Список принятых сокращений

| | |
|---|---|
| АРМ | автоматизированное рабочее место |
| ИБП | источник бесперебойного питания |
| ИСО | интегрированная система охраны |
| ЛВС | локальная вычислительная сеть |
| ПО | программное обеспечение |
| ППКО | прибор приемно-контрольный охранный |
| ППКОП | прибор приемно-контрольный охранно-пожарный |
| ППКП | прибор приемно-контрольный пожарный |
| РД | руководящий документ |
| СВН | система видеонаблюдения |
| СКУД | система контроля и управления доступом |
| СОУЭ | система оповещения и управления эвакуацией |
| СОС | система охранной сигнализации |
| СПС | система пожарной сигнализации |
| ТКП | технический кодекс установившейся практики |
| ТНПА | технические нормативно-правовые акты |
| ТСВ | телевизионная система видеонаблюдения |

## Введение

Вопрос обеспечения безопасности в местах массового скопления людей возникает в каждой крупной организации. В настоящее время в Республике Беларусь возводится большое количество новых бизнес-центров, торгово-развлекательных центров, спортивных сооружений, предполагающих в процессе своего функционирования массовое пребывание в них посетителей и сотрудников. Перед каждым таким объектом возникает задача обеспечения безопасности пребывания людей на его территории. Данная задача может быть сформулирована как на законодательном уровне, так и на уровне руководства объекта.

Для реализации всестороннего обеспечения безопасности используются комплексные интегрированные системы. Каждая из подсистем комплексной системы обеспечения безопасности решает свою задачу, устраняя большинство угроз, исходящих извне. К данным угрозам обобщенно можно отнести угрозу пожара, угрозу несанкционированного проникновения и хищения материальных ценностей и конфиденциальной информации.

Комплексная система безопасности – это совокупность функциональных и информационных связанных друг с другом подсистем безопасности, работающих по одному алгоритму и имеющих общие каналы связи, программное обеспечение, базы данных [1].

Зачастую на объекте устанавливаются неоднородные системы обеспечения безопасности, требующие проведения дополнительной интеграции между собой для обеспечения комплексной защиты и управления системой из единого центра. Способы и методы интеграции подсистем обеспечения безопасности следует выбирать исходя из максимальной эффективности итоговой комплексной интегрированной системы обеспечения безопасности. Вопрос об эффективности системы должен быть проработан на этапе разработки технического решения и должен повлиять на дальнейшую разработку системы обеспечения безопасности в местах массового скопления людей.

При реализации систем безопасности крупных объектов обязательным требованием стала интеграция подсистем между собой с помощью программного обеспечения. Каждая конкретная комплексная система безопасности может изменяться: некоторые подсистемы могут быть исключены или заменены новыми.

Тенденции современного развития систем безопасности неразрывно связаны с процессами широкой автоматизации и интеграции, которые касаются не только систем безопасности, но и всех остальных систем, предназначенных для автоматизации управления жизнеобеспечением и функционированием жилого здания, офиса, предприятия или любого другого объекта.

Применение комплексных интегрированных систем обеспечения безопасности позволит решить огромный круг задач по обеспечению безопасности на объекте с массовым пребыванием людей.

## Лабораторная работа №1. Разработка общей структуры и номенклатуры оборудования системы обеспечения безопасности

**Цель:** разработка структурных схем систем безопасности исходя из имеющейся номенклатуры оборудования.

### 1.1. Современные системы обеспечения безопасности

Установленная комплексная интегрированная система обеспечения безопасности должна обеспечивать следующее:

1. Защиту людей и материальных ценностей от угрозы пожара (пожарная безопасность).

2. Защиту материальных ценностей и конфиденциальной информации от хищения (охрана объекта).

Для решения **задач пожарной безопасности** применяются системы пожарной автоматики. Среди них можно выделить автоматическую систему пожарной сигнализации (СПС), систему оповещения и управления эвакуацией (СОУЭ), систему автоматического пожаротушения и систему дымоудаления.

**Автоматическая СПС** предназначена для выявления факта возникновения возгорания и передачи извещений как другим системам пожарной автоматики и комплексной системы обеспечения безопасности, так и на центральный диспетчерский пункт МЧС. СПС является основной системой пожарной автоматики, так как по ее сигналам принимаются дальнейшие решения по запуску других систем пожарной автоматики. Структура СПС представлена на рис. 1.1 [2].

При обнаружении возгорания пожарным извещателем (ПИ) информация передается по шлейфу пожарной сигнализации на приемно-контрольный пожарный прибор (ППКП). На этапе установки системы в ППКП задается алгоритм реагирования на сообщение о факте возгарания, который включает в себя передачу извещения на пульт централизованного наблюдения (ПЦН) для сообщения о факте пожара в дежурную службу МЧС, а также запуск других систем пожарной автоматики: оповещения и управления эвакуацией, пожаротушения и дымоудаления. При этом автоматическая система пожарной сигнализации также выдает при помощи ППКП сигналы на другие системы обеспечения безопасности и системы управления предприятием, используя интеграционные связи. Характер взаимодействий зависит от производителя приемно-контрольного оборудования и создается, настраивается в процессе выполнения пусконаладочных работ.

Пожарные извещатели в системе пожарной сигнализации организуются в шлейфы. По принципу организации шлейфов СПС можно разделить на пороговые, адресные и адресно-аналоговые [2].

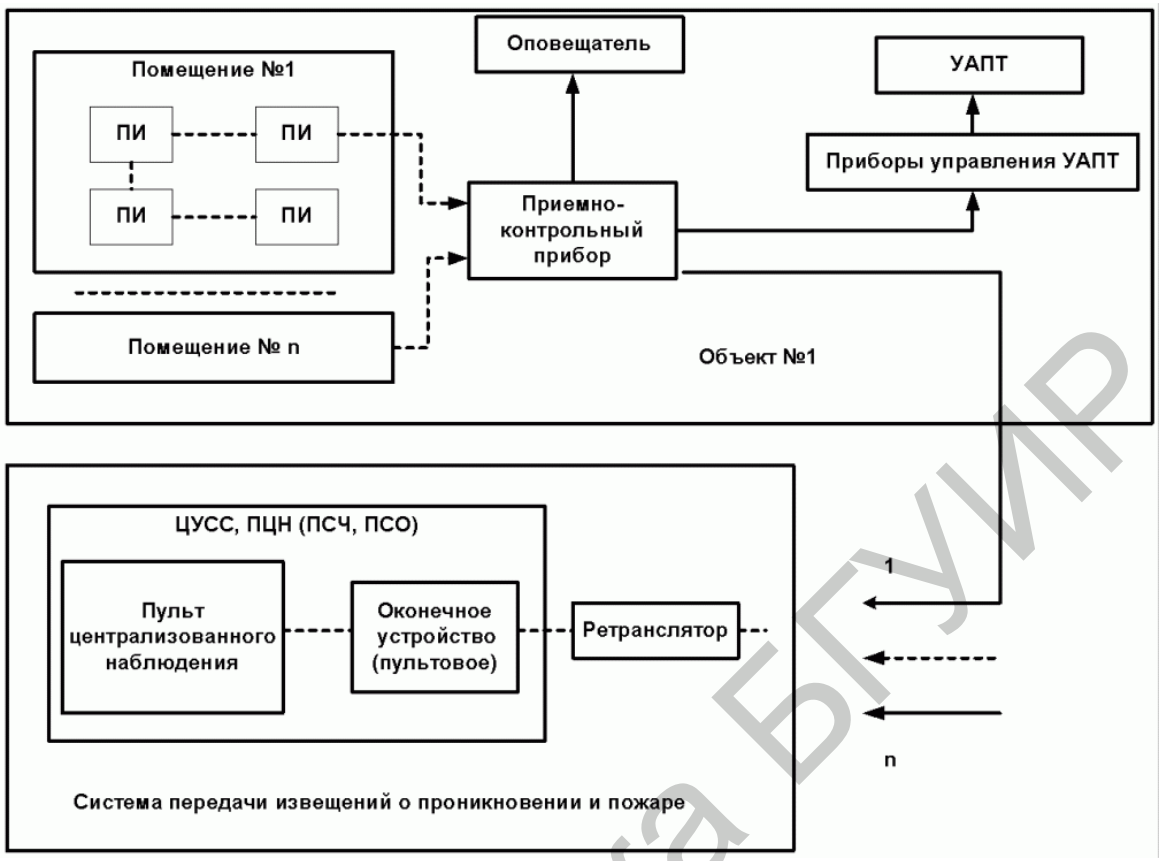


Рис. 1.1. Структурная схема СПС

*Пороговая пожарная сигнализация.* Это наиболее ранний и самый распространенный тип пожарной сигнализации ввиду невысокой стоимости оборудования. В пороговых СПС факт сработки извещателя передается на ППКП путем изменения сопротивления шлейфа, вышедшего за определенный порог. Такой тип систем сильно подвержен ложным срабатываниям, так как передача какой-либо информации практически невозможна, то невозможно определить, является ли факт срабатывания пожарного извещателя ложным под воздействием пыли или других факторов. Защита от их ложных срабатываний обеспечивается за счет увеличения количества извещателей: факт наличия пожара детектируется по одновременному срабатыванию двух пожарных извещателей вместо одного, что приводит к некоторому вынужденному удорожанию системы в целом. Также на уровне ППКП проводятся дополнительные меры по обеспечению защиты от ложных срабатываний, основанные на выдаче извещений о необходимости проведения технического обслуживания. На рис. 1.2 [2] указаны основные пороги, а также постепенное изменение сопротивления дымового шлейфа при запылении.

Тем не менее затраты на монтаж и техническое обслуживание этого типа пожарной сигнализации высоки за счет большого расхода кабельной продукции, а также невысокой надежности извещателей. Принятие решения

о наличии пожара в большей степени зависит от извещателя, а не от прибора. Таким образом, пороговые СПС целесообразно применять на небольших и средних объектах.

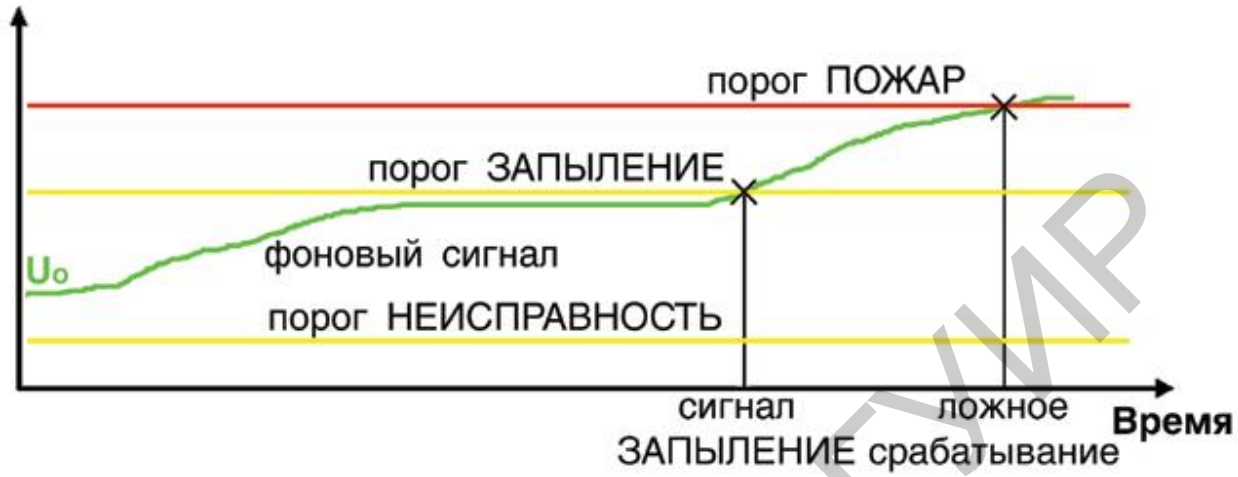


Рис. 1.2. Изменение сопротивления шлейфа пожарной сигнализации во времени

*Адресная пожарная сигнализация*. Появление данного типа пожарной сигнализации было вызвано необходимостью точного определения места возникновения пожара. Каждый извещатель имеет свой адрес или адресную метку и заводскую настройку на один или несколько порогов, позволяет точно определять место возникновения пожара. Но избыточность по количеству извещателей и высокие затраты на обслуживание остаются такими же, как в обычных системах, за счет того что используются пороговые извещатели.

*Адресно-аналоговая пожарная сигнализация*. Самый современный тип пожарной сигнализации. Обеспечивает помимо точного определения места возникновения пожара возможность регистрации его на самой ранней стадии за счет отслеживания не фиксированных порогов, а текущих значений контролируемых параметров. Решение о наличии пожара принимает прибор на основании анализа динамики изменения величины периодически регистрируемых и передаваемых извещателями значений. Данный тип пожарной сигнализации позволяет в зависимости от условий эксплуатации (типов помещений, запыленности извещателей, времени суток и т. д.) программно изменять чувствительность извещателей, устанавливать произвольно пороги срабатывания отдельно для каждого извещателя. Представляют собой систему, гибко подстраиваемую под условия эксплуатации и особенности каждого помещения.

В любом случае СПС должна контролировать каждую точку помещения, где возможно возникновение пожара. В различных помещениях факт наличия пожара требуется устанавливать по разным критериям. В качестве

критерия используется опасный фактор пожара, который детектируется пожарным извещателем. Это может быть дым, тепло, световое излучение пламени, газообразные продукты горения. Для их детектирования используются соответственно дымовой, тепловой, извещатель пламени и газовый пожарный извещатель [3].

**Дымовой пожарный извещатель** реагирует на продукты горения, способные воздействовать на поглощающую или рассеивающую способность излучения в инфракрасном, ультрафиолетовом или видимом диапазонах спектра. Дымовые извещатели могут быть точечными, линейными, аспирационными и автономными. Дымовой пожарный извещатель – наиболее распространенный тип извещателя.

*Точечный* извещатель реагирует на факторы пожара в компактной зоне. Принцип действия точечных оптических извещателей основан на рассеивании серым дымом инфракрасного излучения в дымовой камере (рис. 1.3) [3]. Они хорошо реагируют на серый дым, выделяющийся при тлении на ранних стадиях пожара, и плохо реагируют на черный дым, поглощающий инфракрасное излучение.

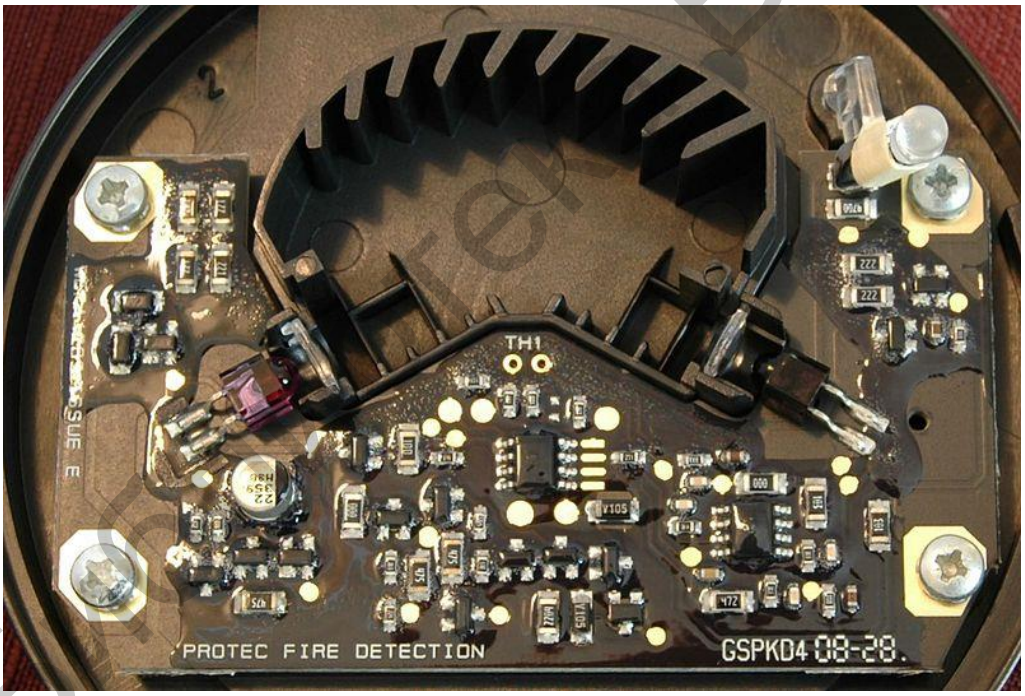


Рис. 1.3. Дымовая камера точечного дымового пожарного извещателя

*Линейный* – двухкомпонентный извещатель, состоящий из блока приемника и блока излучателя (либо одного блока приемника-излучателя и отражателя), реагирует на появление дыма между блоком приемника и излучателя.

Устройство линейных дымовых пожарных извещателей основано на принципе ослабления электромагнитного потока между разнесенными в про-

странстве источником излучения и фотоприемником под воздействием частиц дыма. Прибор такого типа состоит из двух блоков, один из которых содержит источник оптического излучения, а другой – фотоприемник. Оба блока располагают на одной геометрической оси в зоне прямой видимости

*Аспирационный извещатель* – осуществляет принудительный отбор воздуха из защищаемого объема с последующим мониторингом ультрачувствительными лазерными дымовыми извещателями; обеспечивает сверхраннее обнаружение критической ситуации. Аспирационные дымовые пожарные извещатели позволяют защитить объекты, в которых невозможно разместить пожарный извещатель.

*Автономный* – пожарный извещатель, реагирующий на определенный уровень концентрации аэрозольных продуктов горения (пиролиза) веществ и материалов и, возможно, других факторов пожара, в корпусе которого конструктивно объединены автономный источник питания и все компоненты, необходимые для обнаружения пожара и непосредственного оповещения о нем. Автономный извещатель также является точечным. Применение автономных извещателей целесообразно только в бытовых условиях.

Существует также отдельный вид дымового извещателя – радиоизотопный [4]. *Радиоизотопный* извещатель – это дымовой пожарный извещатель, который срабатывает вследствие воздействия продуктов горения на ионизационный ток внутренней рабочей камеры извещателя. Принцип действия радиоизотопного извещателя основан на ионизации воздуха камеры при облучении его радиоактивным веществом. Применение таких извещателей нецелесообразно из-за возможных проблем с радиационной безопасностью, а также повышенных требований к порядку монтажа и технического обслуживания таких извещателей.

*Тепловые пожарные извещатели* в настоящее время применяются в условиях, когда применение дымовых невозможно либо неэффективно. Такие условия могут возникнуть в помещениях с постоянной запыленностью – различные мастерские, помещения кухонь и др. Особенности работы таких извещателей ограничивают площадь их эффективного применения (вдвое по сравнению с дымовыми), а также обеспечивают низкую чувствительность: срабатывание теплового извещателя произойдет в условиях, когда пожар уже в активной стадии и зачастую требует привлечения пожарной бригады для тушения.

*Извещатель пламени* – извещатель, реагирующий на электромагнитное излучение пламени или тлеющего очага [3]. Извещатели пламени применяются, как правило, для защиты зон, где необходима высокая эффективность обнаружения, поскольку обнаружение пожара извещателями пламени происходит в начальной фазе пожара, когда температура в помещении еще далека от значений, при которых срабатывают тепловые пожарные извещатели. Извещатели пламени обеспечивают возможность защиты зон со значительным

теплообменом и открытых площадок, где невозможно применение тепловых и дымовых извещателей.

*Газовый пожарный извещатель* – извещатель, реагирующий на газы, выделяющиеся при тлении или горении материалов. Газовые извещатели могут реагировать на оксид углерода (углекислый или угарный газ), углеводородные соединения. Извещатели такого типа требуют периодической замены чувствительного элемента из-за расхода активного вещества сенсора.

Для решения задач препятствия распространению огня и продуктов горения при уже возникшем пожаре используются системы дымоудаления и пожаротушения.

**Система дымоудаления** – представляет собой специальную приточно-вытяжную систему вентиляции, основными элементами которой являются вентиляторы дымоудаления, противопожарные клапана и огнестойкие воздуховоды [5]. Системы дымоудаления позволяют очистить большие площади от дыма, пепла, гари и мелких частиц, локализуют токсичные вещества, образующиеся при горении искусственных материалов, не давая им распространиться по всему зданию. Помимо этого, локализация дыма и других продуктов горения помогает не допустить повреждения соседних с горящим помещений и минимизировать общие убытки от возгорания.

В целом дымоудаление сочетает в себе комплекс мер, позволяющий управлять перемещением дыма во время пожара, отвести его от путей эвакуации, предотвратить его дальнейшее распространение по зданию и вывести наружу по запланированному маршруту. Для разработки системы дымоудаления учитываются различные факторы – физические свойства материалов конструкции, естественный перепад давлений внутри и снаружи здания, физические свойства дыма и газообразных смесей, образующихся в процессе горения, используются различные методы и специальное оборудование.

Все системы дымоудаления подразделяются на *статические* и *динамические* [5]. При статическом дымоудалении отключаются все вентиляционные системы здания. Отсутствие воздухообмена предотвращает распространение дыма по зданию через вентиляционные шахты и воздуховоды и изолирует продукты горения в одном помещении. Такие системы дымоудаления достаточно просты и недороги.

Более эффективной системой является динамическое дымоудаление (рис. 1.4). При таком методе продукты горения удаляются из помещения при помощи противодымной приточно-вытяжной системы. Она может включать в себя пожарные извещатели, клапаны дымоудаления, огнезадерживающие клапаны, вентиляторы, защитные перегородки, может регулироваться автоматически или вручную.

Основным элементом динамической системы дымоудаления являются вентиляторы дымоудаления [6] – большие термостойкие вентиляторы повышенной мощности с минимальным расходом воздуха от 20 000 м$^3$/ч. Вентиляторы дымоудаления выкачивают дым и продукты горения из зоны возго-

рания и способны эффективно работать даже при самых больших температурах. Вентиляторы дымоудаления могут работать попеременно для отвода дыма и подачи чистого воздуха либо эти функции выполняются ими отдельно. Устанавливаются на крыше здания (рис. 1.5).


Рис. 1.4. Система динамического дымоудаления

Рис. 1.5. Вентилятор дымоудаления

Дымоудаление можно организовать при помощи уже существующих вентиляционных шахт, но наиболее эффективной остается система отдельных коммуникаций, практически исключающая попадание дыма в соседние помещения.

Для обеспечения максимальной пожаробезопасности в зданиях, оснащенных большим количеством инженерных систем и оборудования, рекомендуется использовать автоматические системы управления оборудованием

совместно с системами пожаротушения и дымоудаления. Такой комплекс практически исключает риск возникновения пожара, давая знать о малейших неисправностях оборудования и предпосылках для возникновения аварийных ситуаций. В случаях возгорания автоматические системы пожаротушения и дымоудаления позволяют потушить пожар, избежать человеческих жертв и травм и свести к минимуму материальные потери.

**Системы пожаротушения** предназначены для предотвращения, ограничения развития, тушения пожара с целью защиты от пожара людей и материальных ценностей на объектах.

Наиболее эффективны системы автоматического пожаротушения, которые осуществляют [7]:

– постоянный контроль температуры (или наличия дыма) в охраняемом помещении;

– контроль целостности цепей управления, оповещения, питания;

– выдачу сигнала «Тревога» на пульт централизованного наблюдения;

– включение звуковых и световых оповещателей;

– закрытие огнезадерживающих клапанов;

– включение системы дымоудаления на путях эвакуации людей;

– подачу огнетушащего вещества (ОВ);

– оповещение о факте подачи ОВ.

На рис. 1.6 приведена классификация систем пожаротушения [8].

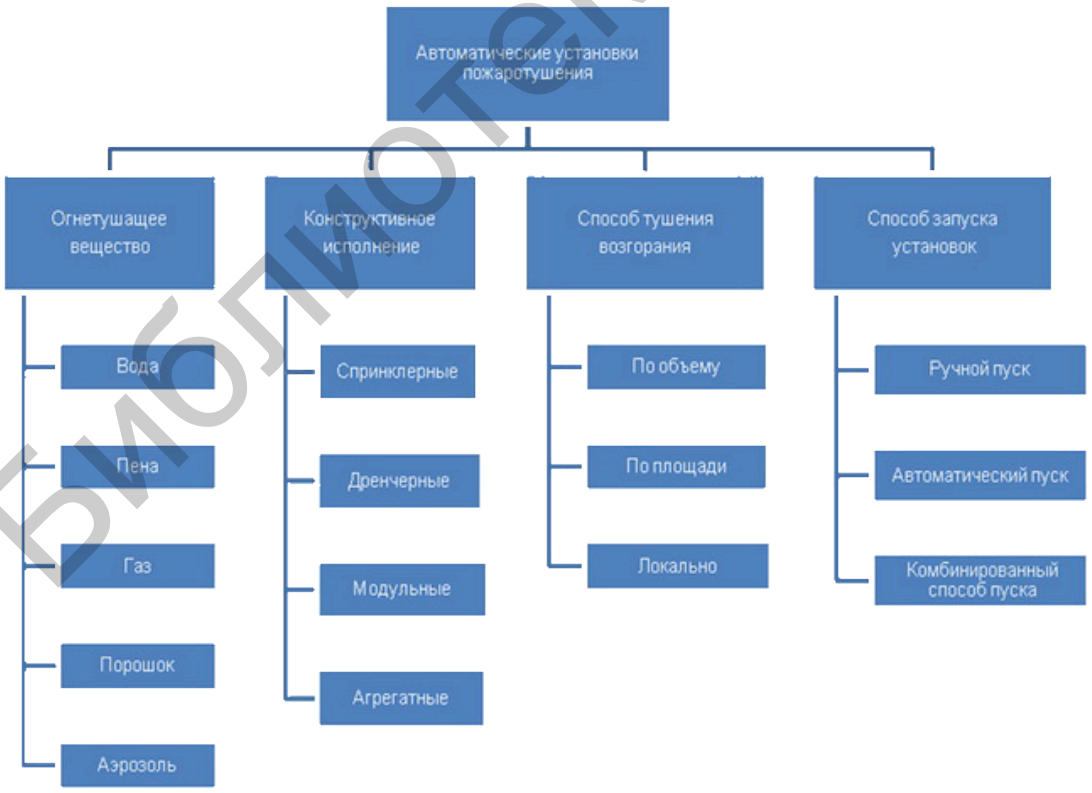


Рис. 1.6. Классификация систем пожаротушения

*Установки водяного пожаротушения* делят на спринклерные, предназначенные для локального тушения пожаров, и дренчерные – для тушения по всей территории или ее части. Спринклерные установки включаются при повышении температуры, при этом струя распыленной воды подается в непосредственной близости от очага пожара. Узлы управления этих установок бывают «сухого» типа – для неотапливаемых объектов и «мокрого» – для помещений, температура в которых в течение года не опускается ниже 0 °С [8].

*Спринклерные установки* в силу своей специфики – низкой чувствительности и независимости (полной или частичной) от пожарной сигнализации – более эффективны для защиты помещений, пожар в которых, скорее всего, будет развиваться быстро, с интенсивным тепловыделением (деревянное помещение и др.). Внешне оросители весьма разнообразны, что позволяет использовать их в различных интерьерах.

*Дренчерные системы* «работают» по команде от извещателя, что позволяет ликвидировать пожар на более ранней стадии развития и быстро.

Сравнительно недавно появились установки пожаротушения *тонкораспыленной водой*. Мельчайшие ее частички обладают высокой проникающей и дымоосаждающей способностью, что усиливает огнетушащий эффект. Получают тонкораспыленную воду за счет значительного повышения давления на распылителях, перегрева воды и других средств.

Общим недостатком установок считается то, что на место пожара подается такое количество воды, которое наносит помещению ущерб, иногда сопоставимый с последствиями пожара [8].

*Установки порошкового пожаротушения* используют в качестве огнетушащего состава специальный порошок. Установки работают как по команде пожарной сигнализации, так и в автономном режиме. В первом случае время подачи огнетушащего вещества на всю защищаемую территорию не превышает 30–35 с после обнаружения опасности. Автономные установки чаще всего выбрасывают разовый заряд порошка и тушат пожар на начальной стадии в локальной зоне, для срабатывания им нужно «дождаться» повышения температуры окружающей среды.

Современные порошки допустимо хранить и применять при температурах до –50 °С, они нетоксичны, мало агрессивны, достаточно дешевы и удобны в обращении. Единственный недостаток порошков – слеживаемость и ограниченный в связи с этим срок хранения. Кроме того, при подаче порошка в зону пожара не исключена полная потеря видимости, поэтому люди из помещения должны быть заблаговременно эвакуированы.

В установках *газового пожаротушения* в качестве огнетушащего вещества в последнее время все чаще используются современные хладоны, газовый состав «Инерген» и другие газы, образующие среду, пригодную для дыхания во время эвакуации людей (тем не менее при большой концентрации вещества людей необходимо эвакуировать). Технология тушения газом

требует, чтобы помещение было герметично закрыто. При хранении газа необходим щадящий температурный режим и контроль за утечкой, чтобы в нужный момент баллоны не оказались пустыми.

*Установки аэрозольного пожаротушения* в качестве огнетушащего вещества используют тонкодисперсный порошок, который образуется в результате горения аэрозолеобразующего состава. Их по понятным причинам нельзя применять в помещениях взрывоопасных категорий. Из-за повышения температуры, давления газовой среды и резкого уменьшения видимости люди должны заблаговременно, еще до включения генератора аэрозоля, покинуть помещение. Сам по себе аэрозоль вредного воздействия на кожу человека и его одежду не оказывает, а его огнетушащая способность велика.

Для решения **задач охраны объекта** применяются системы охранной сигнализации (СОС), системы контроля и управления доступом (СКУД) и системы видеонаблюдения.

**Система охранной сигнализации** по принципу построения и функционирования идентична СПС и зачастую приемно-контрольные приборы имеют возможность функционировать в пожарных и охранных системах и обрабатывать сигналы как пожарных, так и охранных шлейфов.

Условно охранные сигнализации можно разделить на два типа [9]:

1. Автономная система охранной сигнализации. Обеспечивает контроль обстановки на объекте и в случае срабатывания извещателей включает сирену, строб-вспышки и прочие устройства с целью привлечения внимания окружающих.

2. Охранная сигнализация с подключением к пульту централизованного наблюдения (ПЦН). В этом случае при появлении тревожных событий на охраняемом объекте информация от них передается по различным каналам связи на пульт подразделения вневедомственной охраны для оперативного реагирования.

Охрана объектов строится по многорубежной схеме, когда создается два или более рубежа охранной сигнализации, в каждом из которых применяются технические средства, основанные на различных принципах действия.

*Рубеж 1* (периметр) – внешний, наиболее ранний по обнаружению. Этим рубежом блокируются окна, двери, люки, вентиляционные каналы, тепловые вводы, некапитальные стены и другие элементы, доступные для несанкционированного проникновения.

*Рубеж 2* (объем). Второй рубеж предназначен для защиты внутренних объемов помещений. Требования ко второму рубежу охраны в основном сводятся к правильному выбору места установки извещателей, их юстировке и настройке. На особо важных объектах (хранилища в банках, кладовые ценностей, комнатах хранения оружия и т. п.) для охраны отдельных помещений используются несколько извещателей, различных по физическому принципу действия. Особенностью данного рубежа является многочисленность отдель-

ных помещений, общих коридоров и необходимость точного указания помещения, в котором произошла тревога.

*Рубеж 3* (точка). Под точкой понимают локальный объект, материальные ценности, защищаемые охранной сигнализацией. Третьим рубежом блокируются сейфы, металлические шкафы или непосредственно предметы и экспонаты.

Выбор датчиков и извещателей, используемых для всех рубежей охраны, производится с учетом множества факторов: климатических условий, конструктивных особенностей охраняемого объекта, вероятных путей проникновения, режима и тактики охраны.

Охранные датчики (извещатели) бывают нескольких типов, в зависимости от возложенной на них задачи, соответственно в них применяется та или иная технология обнаружения вторжения в охраняемую зону [10]:

– извещатели инфракрасные (объемные);
– магнитоконтактные датчики;
– извещатели разбития стекла;
– извещатели вибрационные;
– извещатели комбинированные;
– извещатели ультразвуковые.

*Инфракрасный извещатель* – это извещатель, который реагирует на изменение уровня теплового излучения при движении человека, предназначен для охраны периметра помещений, коридоров и территории в контролируемой зоне. ИК-датчики являются наиболее распространенными среди всех остальных извещателей, этому способствует простой и надежный метод обнаружения на большой территории охраняемого объекта, а также дешевизна и неприхотливость в работе. Как правило, угол охватываемой зоны составляет около 90°, дальность обнаружения – до 25 м. Некоторые модели игнорируют домашних животных весом до 20 кг, что позволяет использовать данный тип датчиков в квартирах с домашними животными. Часто ИК-извещатели используются с другими охранными датчиками.

*Магнитоконтактный извещатель* (магнитные контакты) применяется для контроля открытия окон и дверей охраняемого помещения [10]. Принцип работы магнитоконтактных датчиков (герконов) основан на взаимодействии магнитов, один из них устанавливается на неподвижную опору, а другой – на подвижную раму окна или двери. Таким образом, контролируется внешний периметр охраняемого помещения, также магнитные контакты можно устанавливать на ворота для дополнительной охраны проезда автотранспорта на территорию. Данный тип датчиков является самым простым и дешевым из всех, но имеет ряд недостатков, например разбитое, но неоткрытое окно или дверь. Герконы используются только как часть полнофункциональной системы охраны и обязательно в комплексе с другими типами охранных извещателей.

*Извещатель разбития стекла* (акустический датчик) реагирует на звук разбития стекла [10]. В памяти извещателя хранятся различные вариации звука разбития различных стекол. Встроенный микропроцессор анализирует звуковой спектр и сличает звук с записанными данными, что позволяет исключить ложное срабатывание извещателя. Радиус действия охранного извещателя разбития стекла составляет около 12 метров, угол реагирования порядка 170°. Такая система надежно защищает от грубого проникновения на охраняемый объект. Акустические извещатели обычно используются совместно с инфракрасными датчиками для повышения надежности всей охранной системы.

*Вибрационные датчики* предназначены для обнаружения преднамеренного разрушения бетонных, кирпичных и деревянных конструкций, а также для обнаружения взлома металлических сейфов [10]. Вибрационные извещатели реагируют на вибрацию на поверхности материала, зона покрытия по бетонной, кирпичной и деревянной поверхности составляет 12 м$^2$, по металлической поверхности – до 6 м$^2$. Современные вибрационные датчики содержат микропроцессор для расширения диапазона обнаруживаемых воздействий (газорежущее, электрорежущее, электродуговое), а также для отсеивания посторонних вибраций.

*Комбинированный извещатель* – это ИК-извещатель и датчик разбития стекла, выполненный в едином корпусе [10]. Комбинированные датчики предназначены для более точного обнаружения нарушителя, исключая «мертвые зоны», также удобны и при монтаже, так как отпадает необходимость устанавливать два разных извещателя. Как правило, такие датчики защищены от радиочастотных излучений и помех, а также от прямого и отраженного света.

*Ультразвуковые датчики* предназначены для обнаружения движения нарушителя в охраняемой зоне в закрытых помещениях [10]. Ультразвуковые извещатели реагируют на движение при возмущении полей упругих волн УЗ-диапазона. УЗ-извещатели применяются в помещениях с уровнем акустических шумов не более 60 дБ и на площади не менее 2×2 м$^2$ (коридор, горячий цех). Данный тип датчиков часто используется с другими извещателями.

*Лучевые датчики* (ИК-барьеры) – это инфракрасные активные двухпозиционные извещатели, состоящие из передатчика и приемника оптического излучения, предназначены для защиты периметра охраняемого объекта [10]. Используются для фиксирования нарушителя на значительном расстоянии, датчики устанавливаются на расстоянии около 60 метров друг от друга, угол настройки 10° – по вертикали, 90° – по горизонтали. Лучевые извещатели являются самым популярным решением для периметральных систем охраны и работают в любых климатических условиях. В современных датчиках существует возможность игнорирования птиц, животных и падающих листьев.

*Емкостные датчики* – это извещатели для охраны сейфов и особо ценных предметов, датчик реагирует на приближение или касание к металличе-

ским предметам [10]. Чувствительность емкостного извещателя настраивается до 20 см. Такие датчики применяются редко, в основном в музеях для охраны экспонатов.

*Датчики с направленной диаграммой обнаружения* – это инфракрасный датчик с установленной линзой [10]. Тип линзы определяется назначением извещателя. Устройство работает по принципу анализа и контроля теплового излучения. Существует несколько видов извещателей с направленной диаграммой обнаружения: штора, завеса, коридор. Этот тип датчиков прост в монтаже, а также эти извещатели устойчивы к ложным срабатываниям.

При срабатывании шлейфа сигнализации ППКО принимается решение о передаче тревожного извещения на ПЦН. Для этого используются промежуточные устройства, обеспечивающие требуемый канал связи.

*Радиопередатчик* передает тревожный сигнал, используя радиоканал. Этот способ довольно универсален, но требуется специальное разрешение на радиочастоту. Да и дальность таких передатчиков ограничена рельефом местности и высотой принимающей антенны. К тому же оборудование довольно дорогое и чувствительно к помехам.

*Автоматический дозваниватель,* используя проводную телефонную линию, оповещает о тревоге. Он передает кодовый тоновый сигнал или заранее подготовленную запись на запрограммированные в него телефонные номера. Это самый надежный и дешевый вариант. Но и у него есть недостатки. Телефонная линия есть не везде, да и из строя ее вывести довольно просто.

С помощью *GSM-модуля* можно оповещать о тревоге посредством коротких SMS-сообщений, используя GSM-канал сотового оператора. Способ простой, но не очень надежный.

Защита любого объекта включает несколько рубежей, число которых зависит от уровня режимности объекта. При этом во всех случаях важным рубежом будет **система управления контроля доступом** (СКУД) на объект.

Хорошо организованная с использованием современных технических средств СКУД позволит решать целый ряд задач [11].

К числу наиболее важных можно отнести следующие:

1) противодействие промышленному шпионажу;

2) противодействие воровству;

3) противодействие саботажу;

4) противодействие умышленному повреждению материальных ценностей;

5) учет рабочего времени;

6) контроль своевременности прихода и ухода сотрудников;

7) защита конфиденциальности информации;

8) регулирование потока посетителей;

9) контроль въезда и выезда транспорта.

СКУД как часть системы безопасности позволяет решить следующие задачи:

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

– предотвращение бесконтрольного проникновения посторонних лиц и транспортных средств на охраняемые территории и в отдельные здания (помещения);

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

– создание надежных гарантий поддержания организационной стабильности внешних и внутренних связей предприятия, отработка механизма оперативного реагирования на угрозы и негативные тенденции;

– пресечение посягательств на законные интересы предприятия, использование юридических, экономических, организационных, социально-психологических, технических и иных средств для выявления и ослабления источников угроз безопасности предприятия.

Все системы контроля и управления доступом можно разделить на четыре класса [11]:

*СКУД 1-го класса* – малофункциональные системы малой емкости, работающие в автономном режиме и осуществляющие допуск всех лиц, имеющих соответствующий идентификатор. В такой системе используется ручное или автоматическое управление исполнительными устройствами, а также световая или/и звуковая сигнализация.

*СКУД 2-го класса* – монофункциональные системы. Они могут быть одноуровневыми и многоуровневыми и обеспечивают работу как в автономном, так и в сетевом режимах. Допуск лиц (групп лиц) может осуществляться по дате, временным интервалам. Система способна обеспечить автоматическую регистрацию событий и автоматическое управление исполнительными устройствами.

*СКУД 3-го и 4-го классов*, как правило, являются сетевыми. В них используются более сложные идентификаторы и различные уровни сетевого взаимодействия (клиент-сервер, интерфейсы считывателей бесконтактных карт или магнитных карт, специализированные интерфейсы и др.).

**Идентификатор пользователя** – это устройство или признак, по которому определяется пользователь [12]. Для идентификации применяются атрибутные и биометрические идентификаторы. В качестве атрибутных идентификаторов используют автономные носители признаков допуска: магнитные карточки, бесконтактные проксимити-карты, брелоки «тач-мемори», различные радиобрелоков, изображение радужной оболочки глаза, отпечаток пальца, отпечаток ладони, черты лица и многие другие физические признаки. Каждый идентификатор характеризуется определенным уникальным двоичным кодом. В СКУД каждому коду ставится в соответствие информация о правах и привилегиях владельца идентификатора.

*Бесконтактные радиочастотные проксимити-карты* (proxmity) – наиболее перспективный в настоящее время тип карт. Бесконтактные карты срабатывают на расстоянии и не требуют четкого позиционирования, что обеспечивает их устойчивую работу и удобство использования, высокую пропускную способность.

*Магнитные карты* – наиболее широко распространенный вариант. Существуют карты с низкокоэрцитивной и высококоэрцитивной магнитной полосой и с записью на разные дорожки.

*Штрих-кодовые карты* – на карту наносится штриховой код. Существует более сложный вариант – штрих-код закрывается материалом, прозрачным только в инфракрасном свете, считывание происходит в ИК-области.

*Ключ-брелок «тач-мемори»* (*touch-memory*) – металлическая таблетка, внутри которой расположен чип ПЗУ.

**Контроллеры** – устройства, предназначенные для обработки информации от считывателей идентификаторов, принятия решения и управления исполнительными устройствами. Именно контроллеры разрешают проход через пропускные пункты. Контроллеры различаются емкостью базы данных и буфера событий, обслуживаемых устройств идентификации.

*Автономные контроллеры* – полностью законченные устройства, предназначенные для обслуживания, как правило, одной точки прохода. Возможность объединения с другими аналогичными контроллерами не предусмотрена. Существует много видов таких устройств: контроллеры, совмещенные со считывателем, контроллеры, встроенные в электромагнитный замок, и т. д.

В автономных контроллерах применяются считыватели самых разных типов. Как правило, автономные контроллеры рассчитаны на обслуживание небольшого числа пользователей, обычно не более 500 человек. Они работают с одним исполнительным устройством без передачи информации на центральный пункт охраны и без контроля со стороны оператора. Примером подобной системы контроля доступа может служить достаточно простая комбинация: «электромагнитный замок + считыватель карт идентификации». Если необходимо контролировать только одну дверь и в будущем расширение системы контроля доступа не планируется, это оптимальное и достаточно недорогое решение.

*Сетевые контроллеры* могут работать в сети под управлением компьютера. В этом случае решение принимает персональный компьютер с установленным специализированным программным обеспечением. Сетевые контроллеры применяются для создания СКУД любой степени сложности. Число сетевых контроллеров в системе может быть от двух до нескольких сотен с обменом информацией с центральным пунктом охраны и контролем, управлением системой со стороны дежурного оператора. В этом случае размеры системы контроля доступа определяются по числу устройств идентификации, а не по числу контролируемых дверей, поскольку на каждую дверь

может быть установлено одно-два устройства идентификации в зависимости от применяемой технологии прохода.

Сетевые СКУД используются на крупных предприятиях и в тех случаях, если нужны ее специфические возможности, такие как учет рабочего времени сотрудников. Сетевые контроллеры объединяются в сеть.

**Устройства идентификации** (считыватели) расшифровывают информацию, записанную на карточках или ключах других типов, и передают ее в контроллер чаще в виде цифровой последовательности. Считыватели карточек доступа могут быть контактные и бесконтактные. Возможны следующие способы ввода признаков [12]:

– ручной, осуществляемый путем нажатия клавиш, поворота переключателей и т. д.;

– контактный – в результате непосредственного контакта между считывателем и идентификатором;

– дистанционный (бесконтактный) при поднесении идентификатора к считывателю на определенное расстояние.

Для съема информации о биологических признаках человека используют специальные биометрические считыватели (терминалы), а ввод ПИН-кода осуществляется с клавиатур различных типов. Именно считыватели определяют внешний вид и основные эксплуатационные характеристики всей системы.

*Кнопочные клавиатуры*. Принцип действия достаточно ясен: если набранный на клавиатуре код доступа верен, то проход на защищаемую территорию разрешен. Кодонаборные устройства иногда совмещаются со считывателем карт, в этом случае код служит для подтверждения факта санкционированного использования карты [12].

*Считыватели штрих-кодов* в настоящий момент практически не устанавливаются в системы контроля доступа, поскольку подделать пропуск чрезвычайно просто на принтере или на копировальном аппарате.

*Считыватели магнитных карт*. Основным элементом считывателя магнитных карт является магнитная головка, аналогичная магнитофонной.

Код идентификации считывается при передвижении карты с магнитной полосой. Основные достоинства таких идентификаторов [12]:

– стоимость считывателей и магнитных карт достаточно низкая;

– возможно изменение кода магнитной карты с помощью кодировщика.

Основные недостатки:

– защищенность от несанкционированного доступа невелика, поскольку нарушитель, завладев на весьма ограниченное время чужой картой, может подделать столько ее дубликатов, сколько ему нужно;

– считыватели магнитных карт достаточно ненадежны в эксплуатации: магнитные головки со временем засоряются и смещаются;

– низкая пропускная способность такой системы контроля доступа, поскольку зачастую приходится идентифицировать магнитную карту несколько раз;

– карты с магнитной полосой требуют весьма бережного хранения, необходимо избегать воздействия электромагнитных полей.

По указанным причинам сложные системы контроля доступа достаточно редко комплектуются подобными устройствами идентификации личности. Магнитные карты метро – исключение из правила, что объясняется дешевизной технологии.

*Считыватели ключей «тач-мемори»*. Считыватель «тач-мемори» крайне прост и представляет из себя фактически контактную площадку, предназначенную для прикосновения специальных ключей. Ключ «тач-мемори» представляет собой специальную микросхему, размещенную в цилиндрическом корпусе из нержавеющей стали.

*Биометрические считыватели*. Проблема исключения подделки и кражи идентификаторов решается путем использования индивидуальных признаков человека – биометрических идентификаторов: отпечатков пальцев, геометрии кисти руки, рисунка радужной оболочки и кровеносных сосудов сетчатки глаза, теплового изображения лица, динамики подписи, спектральных характеристик речи.

Среди **исполнительных устройств** контроля доступа наиболее распространены следующие запорные или управляемые преграждающие устройства: замки, защелки, турникеты (поясные, полноростные, «билетные», раздвижные, вращающиеся трех или четырехштанговые) и шлюзовые кабины (тамбурного типа, ротанты, шлагбаумы), автоматические ворота (распашные ворота, сдвигающиеся ворота, складывающиеся ворота, рулетные ворота), лифты [13]. В современных СКУД применяются в основном электромагнитные и электромеханические замки. Шлюзовые кабины тамбурного типа (две поворотные двери) имеют пропускную способность от 8 до 12 чел./мин. Гораздо выше пропускная способность шлюзов-ротантов, в которых используется только одна поворотная дверь.

*Дверные замки и защелки*. Принцип действия, который используется в электромеханических замках и защелках, весьма прост: при подаче на их специальные контактные клеммы напряжения (обычно в диапазоне 9…16 В) электромагнитное реле притягивает стопор механического устройства, предоставляя возможность открыть дверь.

Мощные штыревые электромеханические замки сейфового типа при подаче напряжения на специальный электромотор осуществляют задвижение запорных штырей внутрь. На строящихся объектах целесообразно использовать именно электромеханические замки, а при необходимости быстро установить систему контроля доступа на действующем объекте лучше применять электромеханические защелки, которые позволяют использовать уже существующие механические замки.

*Электромагнитные замки* состоят из электромагнита, прикрепляющегося к дверной коробке, и ответной металлической пластины, монтируемой на двери. В дежурном режиме на обмотку электромагнита подается постоянный ток удержания, вызывающий сильное магнитное поле, которое притягивает металлическую пластину двери, удерживая ее в закрытом состоянии. При подаче сигнала на специальный вход устройства магнитное поле исчезает и дверь может быть открыта. Все электромагнитные замки характеризуются максимальной механической нагрузкой удержания, которая измеряется в килограммах и может доходить до 1000 кг.

*Шлюзовые кабины* можно разделить на два основных типа, отличающихся устройством, пропускной способностью и ценой: шлюзовые кабины тамбурного типа и шлюзы-ротанты. Шлюзовая кабина тамбурного типа представляет собой замкнутую систему двух зависимых дверей. Основным свойством любой шлюзовой кабины (шлюза) является то, что в любой момент времени открыта только одна из двух дверей.

Принцип действия устройства следующий: человек свободно открывает дверь 1 и входит в шлюз, после чего предъявляет системе контроля доступа свой идентификатор. Если доступ разрешен, открывается дверь 2, а дверь 1 блокируется в закрытом состоянии. Таким образом, гарантируется, что на защищаемую территорию попадет только авторизованный сотрудник. Пропускная способность шлюзовой кабины тамбурного типа находится в пределах от 8 до 12 чел./мин.

Для повышения пропускной способности применяются *шлюзы-ротанты*. Принцип их действия аналогичен шлюзам тамбурного типа, но вместо двух обычных дверей используется одна поворотная дверь турникетного типа. Пропускная способность шлюза-ротанта составляет от 18 до 22 чел./мин. Для более надежной защиты от злоумышленников шлюзы в большинстве случаев комплектуются системами взвешивания для дополнительного контроля количества людей внутри кабины и встроенными металлодетекторами для контроля проноса оружия. Стены кабины могут быть из стали или бронестекла.

*Турникеты* систем контроля доступа также можно разделить на два типа: поясные и полноростовые. Принцип работы турникета достаточно хорошо известен: если запрос на доступ правомерен, то механическая система, поворачиваясь, открывает проход на охраняемую территорию. Турникеты поясные оставляют возможность для перепрыгивания, поскольку, как и следует из их названия, заградительный барьер доходит только до пояса человека, поэтому их целесообразно ставить только рядом с постом охраны.

Турникеты полноростовые можно устанавливать в удаленных от поста охраны местах и использовать в полностью автоматическом режиме работы.

*Автоматические шлагбаумы и автоматика для ворот.* Ворота могут быть распашными (их сопротивление тарану не очень высокое, и они требуют очистки проезжей части перед воротами от снега и льда), раздвижными,

подъемными и рулонными. В качестве атрибутных идентификаторов на транспортное средство применяют путевой лист, в котором указывается государственный номер машины, фамилия водителя и лица, ответственного за перевозку груза (часто эти функции выполняет водитель), вид и количество груза. Идентификаторами водителя и пассажиров являются их пропуска.

Для наблюдения за ситуацией на объекте используются системы видеонаблюдения.

**Видеонаблюдение** (*Closed Circuit Television, CCTV* – система телевидения замкнутого периметра) – процесс, осуществляемый с применением оптико-электронных устройств, предназначенных для визуального контроля или автоматического анализа изображений (автоматическое распознавание лиц, государственных номеров) [14].

В настоящее время существует три типа систем видеонаблюдения, получивших или только получающих широкое распространение:

1) аналоговое видеонаблюдение;

2) IP-видеонаблюдение.

Система аналогового видеонаблюдения появилась изначально, и принципы ее функционирования практически не менялись. Видеокамера формирует аналоговый телесигнал в стандарте PAL или NTSC, видеорегистратор производит оцифровку этого сигнала и запись его на носитель информации.

Система IP видеонаблюдения для передачи сигнала использует протоколы TCP\IP или UDP\IP и передает информацию при помощи сети Ethernet. В данном случае оцифровка сигнала происходит непосредственно в видеокамере, видеорегистратор производит запись и в более сложных системах – анализ и интеллектуальную обработку сигнала.

Видеокамеры систем охранного видеонаблюдения в настоящий момент представлены крайне широким ассортиментом и разработаны для применения в различных условиях, для решения различных задач и имеют различную стоимость. В связи с этим становится актуальной задача правильного выбора видеокамеры для наблюдения в конкретных условиях. Основную роль (не принимая в расчет цену устройства) играет правильный выбор технических характеристик, а также технологий производителя.

К основным параметрам, влияющим на качество получаемого изображения, относятся: тип матрицы, максимальное разрешение, минимальная чувствительность, тип линз объектива, тип исполнения корпуса.

*Тип матрицы*. В настоящее время в видеокамерах устанавливаются матрицы двух типов: ПЗС (CCD) и КМОП (CMOS).

*ПЗС-матрица* (прибор с зарядовой связью) или CCD-матрица (*Charge-Coupled Device*) – специализированная аналоговая интегральная микросхема, состоящая из светочувствительных фотодиодов, выполненная на основе кремния, использующая технологию ПЗС – приборов с зарядовой связью [14]. ПЗС-матрица состоит из поликремния, отделенного от кремниевой подложки, у которой при подаче напряжения через поликремневые затворы из-

меняются электрические потенциалы вблизи электродов. Принцип работы: до экспонирования обычно подачей определенной комбинации напряжений на электроды происходит сброс всех ранее образовавшихся зарядов и приведение всех элементов в идентичное состояние. Далее комбинация напряжений на электродах создает потенциальную яму, в которой могут накапливаться электроны, образовавшиеся в данном пикселе матрицы в результате воздействия света при экспонировании. Чем интенсивнее световой поток во время экспозиции, тем больше накапливается электронов в потенциальной яме, соответственно тем выше итоговый заряд данного пикселя. После экспонирования последовательные изменения напряжения на электродах формируют в каждом пикселе и рядом с ним распределение потенциалов, которое приводит к перетеканию заряда в заданном направлении к выходным элементам матрицы.

*КМОП-матрица* – (комплементарные пары металл-оксид-полупроводник) светочувствительная матрица, выполненная на основе КМОП-технологии [14]. В КМОП-матрицах используются полевые транзисторы с изолированным затвором с каналами разной проводимости. Принцип работы: до съемки подается сигнал сброса, в процессе экспозиции происходит накопление заряда фотодиодом, в процессе считывания происходит выборка значения напряжения на конденсаторе.

*Преимущества КМОП-матриц*:

1. Низкое энергопотребление.

2. Единство технологии с остальными, цифровыми элементами аппаратуры. Это приводит к возможности объединения на одном кристалле аналоговой, цифровой и обрабатывающей, что послужило основой для миниатюризации камер для самого разного оборудования и снижения их стоимости ввиду отказа от дополнительных процессорных микросхем.

3. С помощью механизма произвольного доступа можно выполнять считывание выбранных групп пикселей (кадрирование). Кадрирование позволяет уменьшить размер захваченного изображения и потенциально увеличить скорость считывания по сравнению с ПЗС-сенсорами, поскольку в последних для дальнейшей обработки необходимо выгрузить всю информацию.

4. Усилительные схемы могут быть размещены в любом месте по цепи прохождения сигнала. Это позволяет создавать усилительные каскады и повышать чувствительность в условиях плохого освещения.

5. Дешевизна производства в сравнении с ПЗС-матрицами, особенно при больших размерах матриц.

*Недостатки КМОП-матриц*:

1. Фотодиод ячейки занимает существенно меньшую площадь элемента матрицы по сравнению с ПЗС матрицей, что требует дополнительных технологий и схем для поддержания светочувствительности на уровне ПЗС.

2. Фотодиод ячейки матрицы имеет сравнительно малый размер, величина же получаемого выходного напряжения зависит не только от парамет-

ров самого фотодиода, но и от свойств каждого элемента пикселя. Таким образом, у каждого пикселя матрицы оказывается своя собственная характеристическая кривая и возникает проблема разброса светочувствительности и коэффициента контраста пикселей матрицы.

3. Наличие на матрице большого по сравнению с фотодиодом объема электронных элементов создает дополнительный нагрев устройства в процессе считывания и приводит к возрастанию теплового шума.

*Максимальное разрешение.* Определяет максимальный размер кадра, с которым видеокамера способна выдавать видеоизображение. В аналоговых видеокамерах данное значение не превышает 976×582, что обусловлено требованиями стандарта передачи аналогового видеосигнала PAL и NTSC [15]. Разрешения NTSC (*National Television System Committee* – Национальный комитет по телевизионным стандартам) и PAL (*Phase Alternating Line* – построчное изменение фазы) являются стандартами аналогового видео. Они применяются в сетевом видео, так как видеокодеры способны обеспечивать данные типы разрешения при оцифровке сигнала с аналоговых камер.

В Северной Америке и Японии NTSC является основным аналоговым стандартом, тогда как в Европе и многих азиатских и африканских странах используется стандарт PAL [15]. Оба стандарта возникли в результате развития телеиндустрии. NTSC обладает разрешением в 480 строк, частота обновления равна 60 чересстрочных полей в секунду (или 30 полных кадров в секунду). 480i60 – новое обозначение для данного стандарта, в котором определяется количество строк, тип развертки и частота обновления («i» обозначает чересстрочную развертку). PAL обладает разрешением в 576 строк, частота обновления равна 50 чересстрочных полей в секунду (или 25 полных кадров в секунду). Новое обозначение для данного стандарта – 576i50. Общее количество информации в секунду одинаково для обоих стандартов. При оцифровке аналогового видео максимально возможное количество пикселей основывается на количестве телевизионных строк, доступных оцифровке. Максимальный размер оцифрованного изображения обычно D1, наиболее часто используемое разрешение – 4CIF.

Сетевые IP-видеокамеры способны выдавать разрешение до 50 Мп и более. Наиболее часто востребовано разрешение в 2 Мп (*FullHD*, 1920×1080).

*Минимальная чувствительность*. Определяет наименьшую освещенность, которую сенсор видеокамеры способен уловить как видимый свет, измеряемый в люксах (лк). Современные видеокамеры способны переходить в «ночной» режим, в котором регистрация изображения переключается с цветного на черно-белое, что позволяет увеличить яркость получаемого изображения. Минимальная чувствительность современных видеокамер находится в пределах 0...0,5 лк. При этом чувствительность регистрируется при фиксированном числе диафрагмы. **Число диафрагмы** – значение знаменателя текущего относительного отверстия объектива. Определяется отношением фокусного расстояния к диаметру диафрагмы $f'/D$. Чем выше число диафрагмы,

тем у́же относительное отверстие и тем меньше света попадает на пленку или матрицу. Шкала ирисовой диафрагмы стандартизована и образует следующий ряд: [16]: 1:0,7; 1:1; 1:1,4; 1:2; 1:2,8; 1:4; 1:5,6; 1:8; 1:11; 1:16; 1:22; 1:32; 1:45; 1:64.

*Тип линз объектива.* Определяет, насколько в данной камере возможно максимальное увеличение зоны обзора при помощи оптического зума. Существует три основных типа объектива: фиксированный, вариофокальный и трансфокатор. ***Фиксированный*** объектив обладает фиксированным фокусным расстоянием и не позволяет использовать оптический зум, т. е. размер области, охватываемой камерой, является постоянным. ***Вариофокальный*** объектив позволят при установке камеры настроить область ее обзора, изменяя фокусное расстояние линз на камере. ***Трансфокатор*** обладает механическим устройством регулировки линз и позволяет увеличивать и уменьшать область обзора камеры удаленно при помощи пульта управления. Трансфокатор обладает автофокусом и зачастую используется в поворотных видеокамерах.

*Существуют следующие типы исполнения корпуса видеокамеры*: цилиндрические (*bullet*), в стандартном корпусе (*box*, боксовые), купольные (*dome*), кубические (*cube*), поворотные (скоростные поворотные, *speed dome*, *PTZ*).

***Цилиндрические*** камеры (рис. 1.7) [17] обладают повышенным температурным диапазоном работы и защитой от воздействий окружающей среды (показатель IP65 и выше).

Рис. 1.7. Видеокамера в цилиндрическом корпусе ACTi E39

Видеокамеры в ***стандартном корпусе*** (рис. 1.8) [17] зачастую имеют съемные объективы, что позволяет выбрать объектив самостоятельно в зависимости от поставленной задачи.

Корпус боксовой камеры выполнен с большим количеством щелей и разъемов, что не позволяет использовать ее в условиях улицы без термокожуха – внешней оболочки видеокамеры с функцией подогрева и защитой от окружающей среды (рис. 1.9) [18]. Также боксовые камеры (или камеры в стандартном исполнении) обладают возможностью смены объектива и, как правило, поставляются без него, предоставляя, таким образом, возможность выбора объектива на этапе проектирования на усмотрение проектировщика.

Следует отметить, что подобная возможность выбора объектива в соответствии с требованиями условий размещения видеокамеры позволяет добиться гораздо большего качества изображения, чем при установке видеокамер со встроенными объективами.


Рис. 1.8. Видеокамера в стандартном корпусе ACTi E22

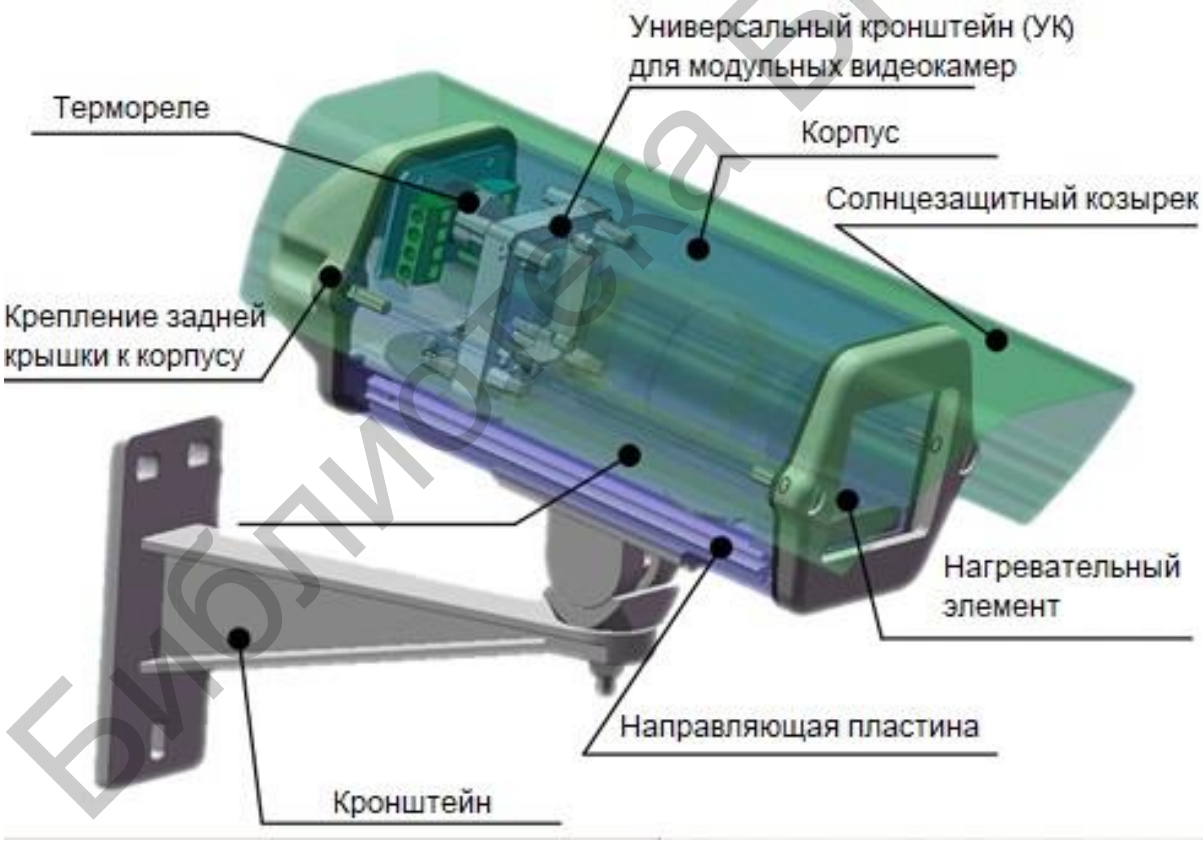


Рис. 1.9. Термокожух *NG-50-135-12*

***Купольные видеокамеры*** (рис. 1.10) [17], благодаря исполнению в виде купола, позволяют увеличить максимальный горизонтальный угол обзора до 90°, а также применять объектив типа «рыбий глаз» с углом обзора до 360°.


Рис. 1.10. Купольная видеокамера ACTi E54

Помимо этого, купольная видеокамера может быть выполнена в антивандальном корпусе (металлический корпус, ударопрочное стекло) и корпусе с защитой от погодных условий и широким температурным диапазоном (рис. 1.11) [17].


Рис. 1.11. Купольная всепогодная видеокамера в антивандальном корпусе ACTi E84

***Кубические*** видеокамеры (рис. 1.12) [17] обладают компактными корпусами, используются только в помещении и обладают наименьшей стоимостью. Ее применение может быть оправдано при необходимости обеспечить видеонаблюдение при небольших затратах и требовании «оригинального» внешнего вида камеры.


Рис. 1.12. Кубическая видеокамера ACTi D22

***Поворотные*** видеокамеры (рис. 1.13) [19] используются для контроля больших площадей помещений или пространств улицы. Могут быть как в уличном, так и внутреннем исполнении, различаясь также максимальным фокусным расстоянием оптики (максимальным оптическим зумом).


Рис. 1.13. Поворотная видеокамера ActiveCam AC-D6034IR10

Помимо основных параметров, существует также ряд **дополнительных** аппаратно-программных технологий и функций, улучшающих изображение в определенных условиях. Среди них можно выделить следующие.

*WDR* (*Wide Dynamic Range* – технология широкого динамического диапазона) – это технология съемки изображений с затемненными участками, при которой затвор диафрагмы открывается дважды [20]. При такой технологии съемки в первый раз используется высокая скорость затвора, затем обычная. Наложив полученные кадры друг на друга, можно получить качественное изображение, на котором нет ни слишком ярких участков, ни затемненных.

*Компенсация заднего света* (*BLC*) – это функция видеокамеры, которая позволяет управлять автоматической регулировкой усиления и электронным затвором не по всей площади экрана, а по его центральной части, что позволяет компенсировать излишек освещения, мешающий восприятию [3]. В некоторых дорогих моделях видеокамер управление электронным затвором происходит по нескольким выбираемым зонам кадра, обеспечивая тем самым наилучшее качество изображения.

Технология *3DNR,* или *3D Noise Reduction,* – эффективный метод подавления шумов в изображении, которые неизбежно появляются при плохом освещении либо в темное время суток [20]. Суть технологии состоит в том, что через определенное заранее время камера проверяет последовательность кадров и перемешивает их. С помощью перемешивания данных на кадре можно подавить большую часть шумов, которые на результирующем изображении уже не будут появляться. Особенно часто эта технология применяется в видеонаблюдении или при съемке фильмов, когда важно подавить шумы и устранить дефекты видео. Правда, данный алгоритм шумоподавления также имеет свои недостатки. При движении в кадре чаще всего появляются дополнительные дефекты и смазывания. Однако если режим шумоподавления включается только для отдельных кадров, то итоговое изображение получается и нешумным, и качественным.

**Видеорегистраторы** (готовые видеосерверы) можно характеризовать по основным и дополнительным параметрам. К основным параметрам можно отнести максимальное количество подключаемых видеокамер, максимальное количество подключаемых жестких дисков, максимальный битрейт, тип поддерживаемого сжатия видеосигнала. К дополнительным можно отнести: максимальное количество подключаемых мониторов, наличие или отсутствие гибридного режима работы, подключение дополнительных устройств и др.

При выборе видеорегистратора требуется руководствоваться маркой выбранных видеокамер. Наилучшую совместимость и качество работы можно достичь, применяя видеокамеры и видеорегистраторы одного производителя.

При использовании интегрированной системы видеоаналитики (Интеллект, TRASSIR, SecurOS, Endura, Axxon Next и др.) нужно учитывать перечень совместимых и интегрированных устройств, размещенный на сайте производителя, и делать выбор в соответствии с этим перечнем.

## 1.2. Анализ методов интеграции и взаимодействия подсистем в комплексной интегрированной системе обеспечения безопасности

При реализации систем безопасности крупных объектов обязательным требованием стала интеграция подсистем между собой. Каждая конкретная КСБ может изменяться: некоторые подсистемы могут быть исключены или заменены новыми.

Основные признаки комплексной системы безопасности.

1. Единая система сбора, обработки и представления данных, мониторинга и управления всеми подсистемами.

2. Возможность задания требуемых сценариев действий любой сложности в ответ на различные события в системе. Под событием в системе понимается все, что происходит в системе: обнаружение движения подсистемой видеоконтроля, тревога датчиков охранно-пожарной сигнализации, факт прохода через двери, контролируемые подсистемой контроля доступа, и т. п. Действием является все, что можно сделать в системе: включить камеру на запись, выдать предупреждение оператору, включить тревожную сигнализацию, поставить/снять датчики с охраны, запретить проход по всем дверям и т. д. В ответ на событие или некий набор событий можно определить любой набор действий системы – сценарий. Более того, применяя специальный язык сценариев, можно определить сколь угодно сложную реакцию системы на события.

3. Возможность интеграции любого оборудования и подсистемы независимо от типа устройств и производителя. Интеграция осуществляется за счет протоколов обмена, программ-драйверов, контроллеров.

4. Модульность и открытые интерфейсы. Система может быть легко расширена как за счет включения новых модулей, так и за счет интеграции системы с уже существующими компьютеризированными системами предприятия. Дополнительные модули могут быть разработаны производителями системы безопасности.

5. Масштабируемость – отсутствие ограничений на масштаб охраняемого объекта и возможность подключения любого количества рабочих мест.

6. Многоуровневая (иерархическая) структура системы позволяет рационально распределить потоки информации между подразделениями предприятия и тем самым минимизировать объем передаваемых данных. Каждое подразделение получает только те сообщения, которые соответствуют служебным обязанностям и уровню ответственности. Тревожное сообщение может быть передано на следующий уровень системы только в том случае, если по истечении допустимого времени отсутствует реакция ответственного персонала [22].

Выделяют три основных типа интеграции подсистем в комплексной системе обеспечения безопасности.

1. Аппаратная интеграция. Представляет собой взаимодействие подсистем на уровне приборов, обычно без использования программного обеспечения. В простейшем случае взаимодействие на аппаратном уровне осуществляется через релейные выходы: реле прибора одной подсистемы воздействует на входы датчиков прибора другой. Например, при срабатывании системы пожарной сигнализации на приемно-контрольном приборе срабатывает специально настроенное реле, замыкающее либо размыкающее контакты на линии пожарной сигнализации контроллера доступа, который, в

свою очередь, переходит в режим пожарной тревоги и открывает свободный проход.

2. Программная интеграция. Представляет собой взаимодействие программных обеспечений подсистем безопасности между собой. Способ программной интеграции применяется в случаях, когда интегрировать системы на аппаратном уровне либо неоправданно сложно, либо нецелесообразно. Как правило, таким путем интегрируются СКУД и системы видеонаблюдения. Взаимодействие подсистем между собой происходит по протоколу TCP/IP посредством локальной сети.

3. Аппаратно-программная интеграция. Представляет собой смешанный случай, когда аппаратное обеспечение одной подсистемы управляется из программного обеспечения другой. Так обычно интегрируются системы видеонаблюдения либо СКУД с системой ОПС. Взаимодействие осуществляется по линиям интерфейсов, используя стандартные протоколы (TCP/IP, Modbus и др.). В этом случае требуются специальные устройства, объединяющие подсистемы, – преобразователи интерфейсов, переходники и др. Пример: интеграция СКУД «Сфинкс» и ОПС «Bolid» (рис. 1.14) [23]. Для интеграции применяется преобразователь интерфейсов Sphinx-Bolid, который позволяет управлять сетью приборов ОПС из интерфейса программного обеспечения СКУД «Сфинкс».

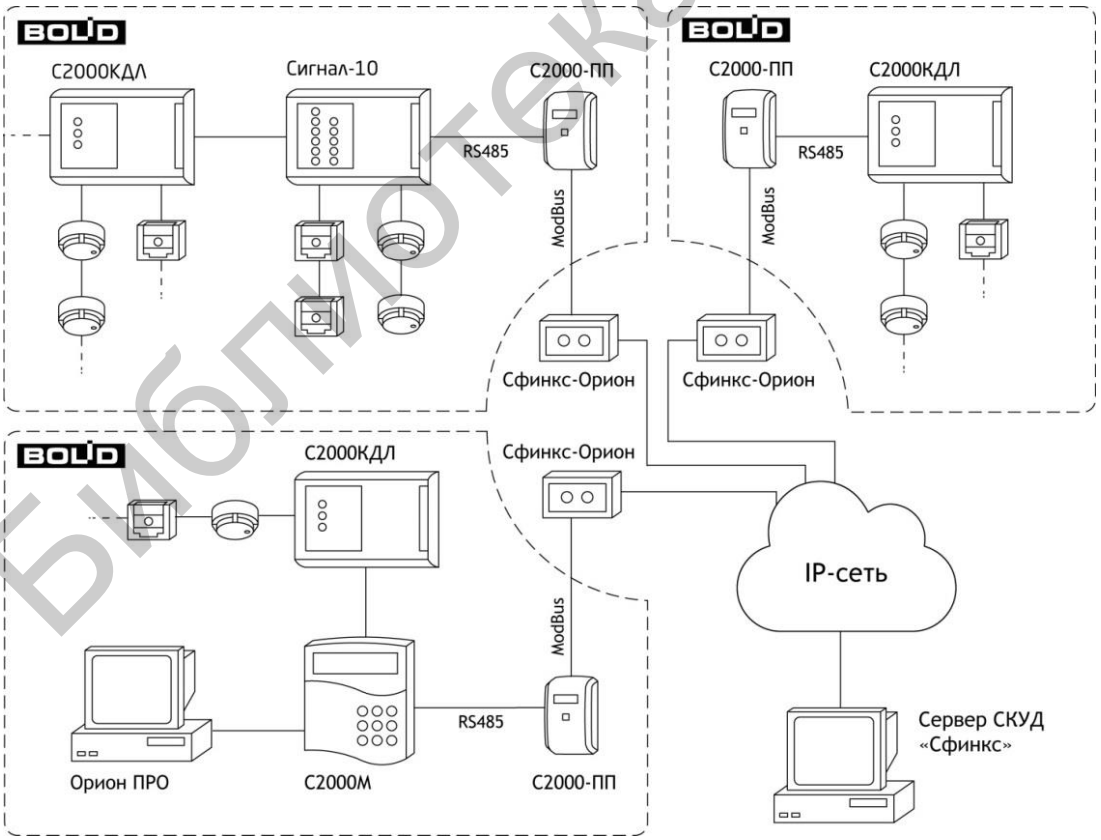


Рис. 1.14. Аппаратно-программная интеграция СКУД «Сфинкс» и ОПС «Bolid»

Наиболее распространенный вариант интеграционных связей, объединяющих подсистемы обеспечения безопасности, следующий.

Системы пожарной автоматики объединяются между собой только при помощи аппаратной интеграции как одной из самых простых и надежных. Реализуется следующий сценарий: срабатывает система пожарной сигнализации. От приемно-контрольного прибора поступает сигнал на прибор системы оповещения и управления эвакуацией, где срабатывает программа эвакуационного оповещения. Включается звуковое сопровождение и объявление о пожаре через громкоговорители системы оповещения. Таким же образом поступает сигнал на пульт МЧС при помощи системы тревожных сообщений по GSM-каналу или телефонии. Далее происходит активация системы дымоудаления, также получившей сигнал от системы пожарной сигнализации. Спустя время, необходимое для эвакуации персонала и рассчитанное на стадии пусконаладочных работ системы, активируется система пожаротушения. В случае спринклерной системы пожаротушения вода начинает поступать сразу же после разбития колбы с термочувствительным раствором на самом спринклере. После отработки всех систем и ликвидации возгорания системы пожарной автоматики требуется выключать вручную.

Помимо интеграции систем пожарной автоматики между собой, требуется обеспечить взаимодействие как минимум с системой контроля и управления доступом. Для этого сигнал от системы пожарной сигнализации поступает на контроллеры или сервер системы контроля и управления доступом, которая открывает точки доступа в свободный режим прохода для обеспечения быстрой эвакуации персонала. В данном случае также целесообразно использовать аппаратную интеграцию на уровне реле из-за высокой надежности и простоты. При приходе сигнала пожарной тревоги на сервер системы контроля и управления доступом создается событие о тревоге, передаваемое в систему видеонаблюдения при помощи связей программной интеграции, которая способна выполнить следующие действия:

1. Используя поступающее изображение с камер наблюдения, оценить его на наличие огня и дыма и вывести данные камеры на весь экран службе охраны, также при этом начать постоянную запись событий.

2. Вывести на экран видеоизображения эвакуационных путей и выходов для возможности управления СОУЭ при использовании СО-4 и СО-5 и начать постоянную запись сигнала с этих видеокамер.

3. Выводить изображение с ассоциированной видеокамеры при вызове с панели обратной связи СОУЭ.

4. Включить постоянную запись с видеокамер, установленных в особо охраняемых помещениях для регистрации возможных действий злоумышленников в сложившейся суматохе.

В другом сценарии при срабатывании системы охранной сигнализации могут быть произведены следующие действия:

1. Сигнал о срабатывании охранной сигнализации передается на пульт централизованного наблюдения департамента охраны и происходит выезд оперативной группы.

2. Система контроля и управления доступом блокирует точки доступа, ведущие в помещение, где сработала сигнализация, с возможностью открытия ответственным охранником.

3. Система видеонаблюдения переводит видеокамеры в режим постоянной записи во всех коридорах и самом помещении, где произошло срабатывание сигнализации и выводит изображение с этих видеокамер на монитор.

Выполнение подобных сценариев с использованием различных методов интеграции позволяет повысить совокупную эффективность систем обеспечения безопасности, повысить возможности управления и контроля за состоянием системы с пульта центрального наблюдения.

### 1.3. Технические нормативно-правовые акты и законодательство Республики Беларусь в области систем обеспечения безопасности

Технические нормативно-правовые акты (ТНПА) определяют требования к системам обеспечения безопасности. Так же как и сами системы, ТНПА определяют требования к пожарной автоматике и охранным системам.

**ТНПА к системам пожарной автоматики** разрабатываются под контролем МЧС Республики Беларусь. В настоящее время действуют следующие основные ТНПА, касающиеся систем пожарной автоматики [24].

СТБ 11.16.04-2009. Система стандартов пожарной безопасности. Системы пожарной сигнализации. Системы пожарной сигнализации адресные. Общие технические условия.

СТБ 11.16.05-2011. Система стандартов пожарной безопасности. Установки аэрозольного пожаротушения автоматические. Генераторы огнетушащего аэрозоля. Общие технические требования. Методы контроля.

СТБ 11.13.19-2010. Система стандартов пожарной безопасности. Установки порошкового пожаротушения автоматические. Модули. Общие технические требования. Методы испытаний.

СТБ 11.13.13-2009. Система стандартов пожарной безопасности. Пенообразователи для подслойного тушения нефти и нефтепродуктов в резервуарах. Общие технические требования и методы испытаний.

СТБ 11.13.05-2009. Система стандартов пожарной безопасности. Генераторы пены низкой кратности для подслойного тушения резервуаров. Общие технические требования и методы испытаний.

СТБ 11.13.07-2009. Система стандартов пожарной безопасности. Генераторы пены низкой кратности стационарные. Общие технические требования и методы испытаний.

СТБ 11.13.06-2009. Система стандартов пожарной безопасности. Генераторы пены средней кратности ручные. Общие технические требования и методы испытаний.

СТБ 2029-2010. Система стандартов пожарной безопасности. Заряды к воздушно-пенным огнетушителям и установкам пенного пожаротушения. Общие технические требования и методы испытаний.

СТБ 11.16.07-2011 (ГОСТ Р 53288-2009). Система стандартов пожарной безопасности. Модульные установки пожаротушения тонкораспыленной водой автоматические. Общие технические требования. Методы испытаний.

СТБ 11.16.06-2011/ГОСТ Р 51043-2002. Система стандартов пожарной безопасности. Установки водяного и пенного пожаротушения автоматические. Оросители. Общие технические требования. Методы испытаний

СТБ 2218-2011. Система стандартов пожарной безопасности. Системы пожарной сигнализации. Извещатели пожарные тепловые. Общие технические требования. Методы контроля.

СТБ 11.14.01-2006. Система стандартов пожарной безопасности. Системы пожарной сигнализации. Приборы управления пожарные. Общие технические условия.

СТБ 11.16.02-2007. Система стандартов пожарной безопасности. Системы пожарной сигнализации. Устройства электроснабжения технических средств противопожарной защиты. Общие технические условия.

СТБ 11.16.03-2009. Система стандартов пожарной безопасности. Системы пожарной сигнализации. Извещатели пожарные дымовые точечные. Общие технические условия.

СТБ 2129-2010. Здания и сооружения. Порядок определения пожарной нагрузки.

НПБ 15-2007. Пожарная автоматика. Область применения.

ТКП 45-2.02-22-2006 (02250). Здания и сооружения. Эвакуационные пути и выходы. Правила проектирования.

ТКП 45-2.02-34-2006 (02250). Здания и сооружения. Отсеки пожарные. Нормы проектирования.

ТКП 45-2.02-190-2010 (02250). Пожарная автоматика зданий и сооружений. Строительные нормы.

ТКП 45-2.02-279-2013 (02250). Здания и сооружения. Эвакуация людей при пожаре. Строительные нормы проектирования.

**ТНПА к системам охраны** разрабатываются под контролем МВД Республики Беларусь. В настоящее время действуют следующие основные ТНПА, касающиеся систем охраны [25].

РД 28/3.001 – 2004. Защитное остекление. Классификация. Методы испытаний. Применение.

РД 28/3.002 – 2004. Роллеты и жалюзи противовзломные и пуленепробиваемые. Классификация. Методы испытаний. Применение.

РД 28/3.003 – 2004. Сейфы и хранилища ценностей. Классификация. Методы испытаний. Применение.

РД 28/3. 004 – 2001. Технические средства и системы охраны. Инструкция о техническом надзоре за выполнением проектных и монтажных работ по оборудованию объектов системами охраны.

РД 28/3. 005 – 2001. Технические средства и системы охраны. Телевизионные системы видеонаблюдения (системы охранные телевизионные). Правила производства и приемки работ.

РД 28/3.006 – 2005. Технические средства и системы охраны. Тактика применения технических средств охранной сигнализации.

РД 28/3. 008 – 2001. Технические средства и системы охраны. Порядок разработки технического задания на проектирование.

РД 28/3. 009 – 2001. Технические средства и системы охраны. Обозначения условные графические элементов систем.

РД 28/3. 010 – 2001. Технические средства и системы охраны. Системы охранной сигнализации. Состав, порядок разработки, согласования и утверждения проектной документации.

РД 28/3. 011 – 2001. Технические средства и системы охраны. Системы контроля и управления доступом. Правила производства и приемки работ.

РД 28/3. 012 – 2005. Требования к технической укрепленности объектов, подлежащих обязательной охране Департаментом охраны Министерства внутренних дел Республики Беларусь.

ТКП 472-2013 (02010). Правила ТО.

ТКП 490-2013 (02010). Правила производства и приемки работ.

СТБ 1250-2000. Охрана объектов и физических лиц. Термины и определения.

Данные ТНПА определяют полный перечень требований к элементам систем, системам в целом, правилам проектирования, монтажа и других аспектов, что позволяет унифицировать системы обеспечения безопасности.

### 1.4. Практическая часть

1. Изучить теоретический материал.

2. Согласно варианту, выданному преподавателем, выполнить техническое задание на проектирование.

3. Исходя из перечня разрешенных к применению технических средств систем безопасности, разработать номенклатуру оборудования, которое предполагается к применению в разрабатываемом варианте задания.

4. Оформить отчет о выполнении лабораторной работы.

## 1.5. Контрольные вопросы

1. Какой ТНПА является основным в части требований к проектам систем пожарной автоматики?

2. Какой ТНПА является основным в части требований к проектам систем охраны?

3. Каков порядок разработки технического задания на проектирование?

4. Перечислите документы, регламентирующие правила производства и приемки работ по системам безопасности.

5. Каковы принципы интеграции систем безопасности и их работа в комплексе.

## Лабораторная работа №2. Разработка технических требований к интегрированным системам обеспечения безопасности

**Цель:** разработка технических требований к проектируемой системе безопасности, размещение компонентов систем безопасности на планах объектов, составление спецификации оборудования и материалов.

### 2.1. Краткие теоретические сведения

Комплексная интегрированная система обеспечения безопасности – совокупность совместно действующих средств (механических, электромеханических, электрических, электронных), обеспечивающих обнаружение проникновения (попытки проникновения) на охраняемые объекты и (или) пожара на них, контроль и управление доступом, а также видеонаблюдение за состоянием охраняемого объекта, связанных между собой аппаратной, аппаратно-программной либо программной интеграцией. Комплексная интегрированная система обеспечения безопасности в общем случае состоит из основных и вспомогательных подсистем. Среди основных подсистем выделяют подсистемы пожарной сигнализации, СОУЭ, системы пожаротушения и дымоудаления, систему охранной сигнализации, СКУД и систему видеонаблюдения. Среди вспомогательных подсистем – система передачи данных, система хранения и система бесперебойного энергоснабжения.

В случае комплексной интегрированной системы безопасности можно выделить и сформулировать требования, включая, но не противореча ТНПА, для применения такой системы в местах массового скопления людей. Стоит отметить, что данные требования в большей степени относятся к системам охраны, так как требования к системам пожарной автоматики достаточно подробно приведены в ТНПА.

### 2.2. Технические требования к основным подсистемам комплексной интегрированной системы обеспечения безопасности

Общие технические требования к **системам пожарной автоматики** регламентируются ТКП 45-2.02-190-2010 [26].

Пожарная автоматика на защищаемых объектах должна быть рассчитана на круглосуточное функционирование и удовлетворять требованиям рациональности, целостности, комплексности, перспективности и динамичности.

*Рациональность* выбираемого варианта пожарной автоматики достигается ее условной оптимизацией, означающей снижение затрат на реализацию при заданной эксплуатационной надежности.

*Целостность* выбираемого варианта пожарной автоматики обеспечивается оптимальным сочетанием и взаимодействием ее составных частей, имеющих ограниченные технические возможности и ресурс.

*Комплексность* выбираемого варианта пожарной автоматики предполагает его сбалансированность с учетом общей целевой задачи при оснащении объекта.

*Перспективность* выбираемого варианта означает, что он должен обеспечивать условия для своего развития с учетом возможных изменений в процессе эксплуатации.

*Динамичность* выбираемого варианта пожарной автоматики заключается в гарантированном выполнении им целевых функций в течение заданного срока службы с учетом износа и восстанавливаемости технических средств.

Пожарная автоматика на защищаемом объекте (в том числе при наличии нескольких зданий и сооружений) должна проектироваться таким образом, чтобы обеспечивалась возможность осуществления централизованного контроля за ее состоянием с общего пожарного поста объекта или другого помещения с наличием круглосуточного дежурства обученного персонала.

Применяемое в составе пожарной автоматики оборудование должно соответствовать эксплуатационным документам на оборудование, требованиям действующих ТНПА, а также обеспечивать работоспособность с учетом климатических, механических, электромагнитных и других воздействий в местах его размещения. Допускается применение в составе пожарной автоматики оборудования разных производителей при его функциональной и технической совместимости в соответствии с характеристиками, указанными в эксплуатационных документах на оборудование.

Тип установок пожаротушения, способ тушения и вид огнетушащего вещества необходимо выбирать с учетом пожарной опасности и физико-химических свойств производимых, хранимых и применяемых веществ и материалов, а также объемно-планировочных, конструктивных и технологических особенностей защищаемого объекта.

Пожарная автоматика должна обеспечивать автоматическое отключение технологического, электротехнического и другого оборудования в случаях, когда его работа может привести:

– к снижению эффективности работы СПС или установок пожаротушения;

– к распространению пожара и продуктов сгорания;

– к поражению людей электрическим током, сильнодействующими ядовитыми веществами;

– к взрыву, аварии, повреждению данного оборудования под воздействием огнетушащего вещества.

Не допускается применение установок объемного пожаротушения (кроме установок пожаротушения тонкораспыленной водой) в помещениях,

которые не могут быть покинуты людьми до начала работы установок пожаротушения.

Также следует отметить требования НПБ 15-2007 [27], согласно которым в местах массового скопления людей требуется предусматривать адресную систему пожарной сигнализации благодаря ее более гибкой настройке, точному определению неисправности и пожарной тревоге.

**Системы охранной сигнализации** подпадают под требования РД 28/3.006 – 2005 и ТКП 490-2013 (02010) [28].

Основной принцип, который должен соблюдаться при проектировании и монтаже систем охранной сигнализации, состоит в обязательном оснащении техническими средствами охранной сигнализации всех уязвимых мест объекта, защищаемого с помощью системы охранной сигнализации.

Обязательным условием обеспечения повышенного и высокого уровней защиты объектов (помещений) подгрупп AI, AII и БII должно являться наличие многорубежной системы охранной сигнализации.

Рубежи охранной сигнализации включают в себя извещатели для блокировки строительных конструкций периметра объекта (1-й самостоятельный рубеж), объема и площадей объекта (2-й самостоятельный рубеж), мест непосредственного хранения ценностей (3-й самостоятельный рубеж).

Для создания первого рубежа сигнализации должны использоваться омические (одножильный провод типа НВ, ПЭЛ, фольга), вибрационные (типа «Vibro», «ES-400», «Грань-2», «Шорох-1», «Шорох-1-1»), сейсмические (типа «GM-530», «GM-560»), трибоэлектрические (типа «Градиент», «Гюрза 048 П»), пассивные звуковые для блокировки остекленных конструкций (типа «FG-730», «FG-1025», «Лира», «ИНС-206», «Авант-211», «Авант-Glasstrek», «Glasstech»), совмещенные (типа «Филин-1», «Филин-2», «ИНС-408», «SPRG-1»), поверхностные пассивные оптико-электронные инфракрасные (типа «ИНС-102», «СН-1000», «Clip-1») извещатели для блокировки дверей, стен, полов, потолков, остекленных конструкций на пролом и разрушение; магнитоконтактные извещатели для блокировки дверей и окон на открытие, стекол на выем, а также омические и вибрационные – для блокировки вентиляционных каналов, коробов.

Для создания второго рубежа сигнализации должны использоваться объемные пассивные оптико-электронные инфракрасные извещатели (типа «ИОН», «ИНС-101», «ИНС-103», «АВАНТ-Bravo L1», «АВАНТ-Bravo L2», «Colt XS», «Jet»), ультразвуковые (типа «Эхо-А», «Эхо-2», «Эфа», «Microsonic», «US-10»), радиоволновые доплеровские (типа «Аргус-3», «Волна-5»), электростатические (типа «Гюрза-027П») или комбинированные (типа «DT-7235», «ИНС-307», «SRX-1000») извещатели.

Для третьего рубежа сигнализации при блокировке сейфов, металлических ящиков должны использоваться магнитоконтактные извещатели совместно с емкостными (типа «Пик», «Риф-М»), вибрационными пьезоэлектрическими (типа «Vibro», «ES-400», «Грань-2», «Шорох-1»), сейсмическими

(типа «GM 530», «GM 560») или объемными извещателями. Для блокировки ценных предметов (картин, икон и т. п.) должны использоваться объемные пассивные оптико-электронные инфракрасные извещатели, вибрационные пьезоэлектрические извещатели с выносными чувствительными элементами типа «Гюрза-050 П».

Размещение и установка средств *систем контроля и управления доступом* строго не регламентируются и подпадают лишь под общие требования электробезопасности. Следует сформировать следующие общие требования к СКУД.

СКУД в местах массового скопления людей должны обеспечивать ограничение доступа посторонних лиц в служебные и технические помещения объекта с достаточной эффективностью.

В зависимости от типа точек доступа требуется устанавливать соответствующие преграждающие устройства:

– на проходных, предназначенных для доступа персонала на территорию объекта, с наличием охранника устанавливаются полуростовые турникеты для прохода людей и автоматические шлагбаумы для проезда автомобилей;

– на проходных, предназначенных для доступа персонала на территорию объекта, без постоянного охранника устанавливаются полноростовые роторные турникеты для прохода людей и автоматические ворота для проезда автомобилей;

– на дверях между помещениями для доступа из коридора требуется устанавливать электромеханические замки или защелки. При этом обязательно требуется установка дверного доводчика.

Тип электрических замков или защелок должен выбираться в зависимости от их наработки на отказ и числа пользователей [29]. Выбор типов доводчиков двери должен производиться с учетом максимального веса двери (усилия). Не допускается установка доводчиков на двери, вес которых превышает допустимый вес, при котором доводчик гарантированно выполняет свои функции.

Для доступа в особо важные помещения требуется устанавливать шлюзы с обязательной видеофиксацией входящего человека.

Согласно РД 28/3. 011 – 2001 [29] также требуется следующее:

– средства КУД должны в обязательном порядке иметь резервное электропитание при пропадании основного источника электропитания; переход на резервное питание и обратно должен происходить автоматически без нарушения установленных режимов работы и функционального состояния СКУД;

– при использовании в качестве резервного источника питания аккумуляторной батареи должна обеспечиваться работа средств КУД в течение не менее 8 ч, а также выполняться автоматическая подзарядка аккумулятора.

Программное обеспечение СКУД должно:

1) выполнить полную регистрацию всех событий системы;

2) иметь возможность анализа и составления отчетов по событиям системы;

3) осуществлять учет рабочего времени сотрудников;

4) иметь возможность интегрироваться с системами видеонаблюдения и пожарной автоматики;

5) выводить информацию о проходах в реальном времени на монитор оператора;

6) осуществлять мониторинг состояния компонентов и устройств системы;

7) иметь возможность удаленного администрирования и конфигурирования;

8) осуществлять реакцию на события как от контроллеров системы, так и от других систем обеспечения безопасности;

9) автоматически производить резервное копирование базы данных;

10) иметь возможность управления режимами доступа персонала через точки доступа по времени суток, дням недели и месяца и т. д.

Таким образом, СКУД должна иметь широкие возможности по разграничению доступа, гибкую настройку и полностью информировать администратора системы и ее пользователей о всех событиях.

На *систему видеонаблюдения* в настоящее время возложены не только задачи наблюдения за территорией объекта, но и аналитические функции, возможность построения комплексной системы обеспечения безопасности на базе видеосервера. Исходя из этих задач сформулируем следующие требования:

1) СВН должна осуществлять непрерывную передачу изображения с видеокамеры на пост дежурного охранника;

2) вести архив видеонаблюдения на базе подсистемы хранения данных;

3) производить аналитику изображения с видеокамер с целью увеличения скорости работы оператора системы, регистрации тревожных событий и передачи данных в базу данных;

4) интегрировать в себя системы контроля и управления доступом, системы охранно-пожарной сигнализации;

5) иметь возможность гибкой реакции на события любой интегрированной системы безопасности;

6) управлять (по мере необходимости) техническими средствами интегрированных систем обеспечения безопасности.

Также на законодательном уровне к СВН были предъявлены требования Постановлением Совета Министров Республики Беларусь от 11 декабря 2012 г. №1135 [30], среди которых можно выделить нижеследующие.

1. Средствами, используемыми для создания телевизионных систем видеонаблюдения, обеспечиваются:

– передача видеоизображения в режиме реального времени;

– синхронизация событий с системой единого точного времени;

– использование основного транспортного протокола передачи информации TCP/IP;

– защищенный доступ к настройкам устройства;

– работа в широком диапазоне температур (от –30 до +40 °С) в круглосуточном режиме – при расположении вне отапливаемых или кондиционируемых помещений;

– поддержка спецификаций ONVIF;

– передача оцифрованного видеосигнала в форматах MPEG-4 и (или) H.264.

2. Видеокамеры, используемые в системах безопасности и телевизионных системах видеонаблюдения, должны иметь:

– индивидуальную настройку параметров изображения (яркость, цвет, контраст) и при необходимости – временный интервал записи предтревоги и посттревоги;

– разрешение изображения не менее 720×576 пикселей (4CIF) – для стационарных камер при размещении внутри зданий и сооружений и не менее 1280×1024 пикселей при наружном размещении.

3. Для обеспечения функционирования указанных видеокамер по возможности используется электропитание в соответствии со стандартом PoE (питание через Ethernet).

4. Для наружного наблюдения используются видеокамеры, имеющие высокую чувствительность (не ниже 0,5 лк – для хорошо освещенных участков местности, не ниже 0,05 лк и с применением инфракрасной или иной подсветки – для плохо освещенных участков местности).

5. Разрешающая способность видеокамер на границах контролируемой зоны задается в следующих пределах:

– не менее 150 пикселей на метр (далее – пикс/м) – для узнаваемости внешности человека (в местах массового скопления людей);

– не менее 250 пикс/м – для идентификации внешности при входе в помещение и выходе из него и в местах, где проход граждан ограничен;

– не менее 50 пикс/м и с частотой кадров не менее 25 кадров в секунду, если иное не установлено законодательными актами, – для распознавания событий (действий человека, воздействия на объекты, качественного изменения объектов).

6. Серверами видеоархивов обеспечиваются:

– возможность выборки видеоинформации по заданным временным параметрам для ее просмотра, копирования и воспроизведения;

– авторизация и регистрация всех пользователей системы по именам, паролям, времени работы, а также разграничение пользователей и прав доступа к функциям системы;

– циклическая запись видеоинформации от видеокамер в видеоархив с качеством, пригодным для идентификационных исследований, с привязкой видеозаписей ко времени и видеокамере и с защитой от редактирования.

7. Срок хранения видеоархива (время цикла обновления) не менее 30 сут; санкционированный доступ к видеоархиву с рабочего места оператора, удаленного компьютера.

### 2.3. Технические требования к вспомогательным подсистемам

К вспомогательным подсистемам комплексной системы обеспечения безопасности следует отнести систему бесперебойного питания, систему передачи данных, систему хранения.

Основными задачами **источников бесперебойного питания** (ИБП) в системе бесперебойного питания являются [31]:

– обеспечение питания ответственных потребителей на время не менее заданного времени (обычно 30 мин) при нарушениях в работе электрической сети;

– повышение качества электрической энергии, получаемой от питающей сети и поступающей к ответственным потребителям;

– создание гальванической развязки электрической сети.

ИБП в составе систем бесперебойного питания должны:

1) работать в широком диапазоне изменения входного напряжения (не менее ±15 %);

2) иметь как можно более близкое к единице значение коэффициента входной мощности, что позволяет наиболее корректно работать совместно с дизель-генераторными установками;

3) иметь высокую перегрузочную способность (не менее 200 % в течение 1 мин и 125 % в течение 10 мин) и устойчивость к большим фазовым перекосам;

4) иметь коэффициент гармонических искажений на входе не более 8 %;

5) иметь КПД не ниже 92–94 %;

6) иметь в своем составе (или иметь возможность подключить) разделительный трансформатор;

7) иметь возможность параллельного включения однотипных систем;

8) при переходе на питание от аккумуляторной батареи переключаться без разрыва синусоиды (система онлайн);

9) иметь удобную и гибкую систему управления;

10) использовать высококачественные герметичные необслуживаемые свинцово-цинковые кислотные аккумуляторные батареи со сроком службы до 10 лет;

11) обладать развитым программным обеспечением (мониторинг, автоматическое управление локальной вычислительной сетью, удаленное оповещение, безопасное отключение);

12) быть удобными в обслуживании и ремонте.

Оборудование системы бесперебойного питания требуется устанавливать централизованно с целью облегчения доступа, обслуживания и возможности защиты от несанкционированного доступа.

Следует отметить, что производители серверного оборудования также самостоятельно производят и системы бесперебойного питания для них, подбираемые в каждом конкретном случае самим производителем, однако для решения широкого профиля задач используются ИБП сторонних производителей. Наиболее распространенными являются ИБП американской корпорации *APC*, отличающиеся универсальностью применения, высоким качеством, удобством в подборе и эксплуатации.

**Подсистема передачи данных** характерна для сетевых систем обеспечения безопасности и представляет собой линии и устройства передачи и (или) преобразования сетевых сигналов. Наиболее часто такой системой является локальная вычислительная сеть (ЛВС), построенная на базе стандарта Ethernet. Реже применяется сеть на базе промышленного интерфейса RS-232 или RS-485. Среди компонентов подсистемы передачи данных можно выделить следующее сетевое оборудование: сетевые коммутаторы, маршрутизаторы, модемы, преобразователи интерфейсов, беспроводные точки доступа.

Виды сетей передачи данных:

1) локальные вычислительные сети (ЛВС) любой сложности;

2) территориально-распределенные вычислительные сети, – объединение нескольких ЛВС, расположенных на территории предприятия;

3) глобальные вычислительные сети – объединение ЛВС нескольких филиалов и предприятий корпорации;

4) беспроводные технологии ЛВС и линий связи;

5) системы передачи данных и удаленного доступа с использованием DSL-оборудования;

6) беспроводные локальные сети и зоны Wi-Fi стандарта группы IEEE 802.11.

Для удовлетворения современных требований к сетевой инфраструктуре она должна поддерживать следующие сетевые приложения и сервис:

– интегрированная передача голосовых, видео- и цифровых данных;

– создание виртуальных локальных и частных сетей;

– управление сетью на основе правил;

– использование соглашений об уровне предоставляемых услуг;

– учет используемых ресурсов;

– управление пользователями;

– функционирование приложений, требующих передачи многоадресного трафика;

– построение сетей Internet, Intranet, Extranet.

В настоящее время наиболее распространены сетевые коммутаторы, поддерживающие следующие физические интерфейсы Ethernet [32].

*10BASE-T* – для передачи данных используется четыре провода кабеля витой пары (две скрученные пары) категории 3 или категории 5. Максимальная длина сегмента 100 м. Используется для связи с сетевыми контроллерами СКУД.

*100BASE-TX* – развитие стандарта 10BASE-T для использования в сетях топологии «звезда». Задействована витая пара категории 5, фактически используются только две неэкранированные пары проводников, поддерживается дуплексная передача данных, расстояние до 100 м. Используется для связи с IP-видеокамерами СВН.

*1000BASE-T* – стандарт, использующий витую пару категории 5е. В передаче данных участвуют четыре пары. Скорость передачи данных 500 Мбит/с по одной паре. Используется метод кодирования PAM5, частота основной гармоники 62,5 МГц. Расстояние до 100 м. Используется для связи между коммутаторами и сервером СВН.

Сетевые коммутаторы, использующиеся в системах IP-телефонии, системах охранного видеонаблюдения должны поддерживать технологию *Power over Ethernet* (*PoE*), описываемую стандартами IEEE 802.3af-2003 и IEEE 802.3at-2009 [33]. PoE – технология, позволяющая передавать удаленному устройству электрическую энергию вместе с данными через стандартную витую пару в сети *Ethernet*. Данная технология предназначается для IP-телефонии, точек доступа беспроводных сетей, IP-камер, сетевых концентраторов и других устройств, к которым нежелательно или невозможно проводить отдельный электрический кабель.

Для целей создания интеграционных связей, а также управления оборудованием часто применяются специальные устройства – преобразователи интерфейсов

*Преобразователи интерфейсов* – устройства преобразования формата передаваемых данных для передачи их по другому (отличному от первичного) интерфейсу. Преобразование данных происходит на программном уровне. Помимо непосредственно изменения структуры передаваемых данных, программная составляющая преобразователя интерфейсов отвечает за определение типов протоколов, используемых в системе, и выбор алгоритма для их согласования. Как правило, в системах обеспечения безопасности используются несколько типов преобразователей интерфейсов.

1. Преобразователь RS-232 – RS-485/422. Используется для совместного функционирования устройств, использующих промышленные интерфейсы.

2. Преобразователь RS-232 (422, 485) – Ethernet. Используется для управления устройствами, подключенными по промышленному интерфейсу

через ЛВС. Как правило, такие преобразователи имеют веб-интерфейс, посредством которого происходит их настройка и управление.

3. Преобразователь RS-232 (422, 485) – USB. Используется для управления устройствами, подключенными по промышленному интерфейсу через USB-порт компьютера.

Зачастую производители оборудования систем безопасности производят также и преобразователи интерфейсов, учитывающие особенности взаимодействия устройств и сервера, а также гарантированно поддерживаемые собственным программным обеспечением систем безопасности.

**Подсистема хранения данных** – комплекс устройств, обеспечивающих хранение и резервирование данных. Наиболее распространены *NAS* (*Network Attached Storage*) – сетевая система хранения данных, сетевое хранилище. По сути представляет собой компьютер с некоторым дисковым массивом, подключенный к сети (обычно локальной) и поддерживающий работу по принятым в ней протоколам. Часто диски в NAS объединены в RAID-массив. Несколько таких компьютеров могут быть объединены в одну систему [34].

В настоящее время выпускаются законченные NAS-устройства, обладающие необходимыми для функционирования NAS параметрами, однако полноценными компьютерами не являющиеся. Такие устройства носят название *дисковый массив*. В отличие от отсека для установки жесткого диска в корпусе компьютера или специального конструктива для крепления одиночного диска, включающего в себя средства реализации физического и механического (соответствующие разъемы) интерфейса и при необходимости крепежа внутри такого конструктива дискового накопителя иного формата (например, 3½″ в конструктиве 5¼″), так называемого «кармана», дисковый массив представляет собой куда более сложную систему, состоящую из следующих компонентов:

1) контроллеры, обладающие способностью виртуализации и способные создавать RAID;

2) кэш-память (в зависимости от конструкции может быть как на борту контроллера, так и отдельным конструктивом дискового массива);

3) блоки питания (промышленные дисковые массивы имеют избыточное резервирование блоков питания);

4) отдельное резервное питание для контроллера и кэш-памяти;

5) средства охлаждения дисков и контроллеров, вентиляторы и т. д;

6) контроллеры доступа потребителей к дисковому пространству: FC, SCSI, Ethernet;

7) корзины для дисков (блоками на несколько дисков или отдельные диски);

8) собственно сами диски.

Некоторые из этих блоков могут быть выполнены в виде единой платы, например: RAID-контроллером, вместе с кэш-памятью, резервным питанием

кэша и контроллером доступа. Также в некоторых менее дорогих устройствах могут отсутствовать какие-то компоненты или их резервирование.

Обычно дисковый массив обеспечивает высокую доступность благодаря:

1) резервированию избыточными компонентами: диски, блоки питания;

2) резервированию путей доступа к дисковому массиву: Multipat;

3) возможности горячей замены.

Также дисковые массивы могут обеспечивать повышенную скорость доступа к данным или увеличенную пропускную способность благодаря кэш-памяти, использованию RAID, балансировке нагрузки на контроллере средствами технологии Multipath, предикативному чтению.

Дисковые массивы условно подразделяются на три класса [35].

*Entry-level* – начальный уровень. Для домашнего пользования и малого бизнеса. Устройства Entry-level, как правило, состоят из небольшого (несколько единиц) количества дисков и либо имеют один контроллер либо не имеют его вообще. Обычно реализованы в настольном исполнении либо в виде одной дисковой полки. Батареи резервного питания, как правило, не имеет.

*Mid-Range* – средний уровнь. Для небольших организаций и подразделений предприятий. Устройства Mid-Range обычно имеют модульную конструкцию и состоят из одной или нескольких (до нескольких десятков) дисковых полок, монтируемых в стойку. Характеризуются наличием двух аналогичных контроллеров, каждый из которых имеет свою кэш-память и обслуживает часть дисков и серверных подключений. Имеет дублированные компоненты электропитания и вентиляции, а также резервную батарею. Не имеет единой точки отказа. В случае выхода одного из контроллеров сохраняется доступ ко всей хранимой информации, но утрачивается половина производительности.

*Hi-End, или Enterprise,* – уровень предприятия. Сюда относятся массивы высшего класса для использования крупными предприятиями. Имеют высшую по сравнению с предыдущими классами производительность и надежность. Как правило, обладают следующими характеристиками:

– монолитная или монолитно-модульная конструкция в виде отдельно стоящего шкафа (шкафов);

– возможность установки от сотни до тысяч дисков;

– симметричная мультипроцессорная архитектура;

– имеет до нескольких десятков специализированных контроллеров, каждый из которых предназначен либо для дисковых (*BackEnd*) либо для хостовых (*FrontEnd*) операций.

Контроллеры разделяют общую память. Устройство полностью резервировано. При выходе из строя любого из компонентов (в том числе диска, контроллера) падение производительности незначительно (менее половины).

Особенностью Hi-End систем является поддержка оборудования Mainframe, в том числе интерфейсов ESCON, FiCON.

При объединении дисков в дисковом массиве зачастую используется *RAID* (*Redundant Array of Independent Disks*) – массив из нескольких дисков (запоминающих устройств), управляемых контроллером, связанных между собой скоростными каналами передачи данных и воспринимаемых внешней системой как единое целое. В зависимости от типа используемого массива возможно обеспечивать различные степени отказоустойчивости и быстродействия. Служит для повышения надежности хранения данных и/или для повышения скорости чтения/записи. Существуют следующие типы RAID-массивов [36].

*RAID 0* – дисковый массив повышенной производительности с чередованием без отказоустойчивости. Информация разбивается на блоки данных фиксированной длины и записывается на оба/несколько дисков одновременно (рис. 2.1) [36].

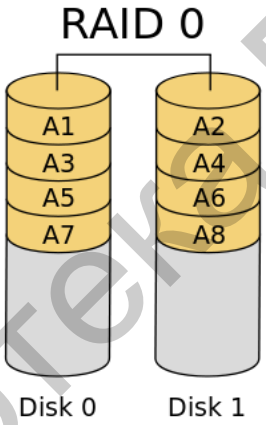


Рис. 2.1. Схема RAID 0

*Достоинства:*

1. Существенно повышается производительность (от количества дисков зависит кратность увеличения производительности).
2. Объем памяти суммируется.

*Недостаток:* надежность RAID 0 меньше надежности самого ненадежного диска, так как отказ любого из дисков приводит к неработоспособности всего массива.

*RAID 1* – зеркальный дисковый массив. Это массив из двух дисков, являющихся полными копиями друг друга (рис. 2.2) [36].

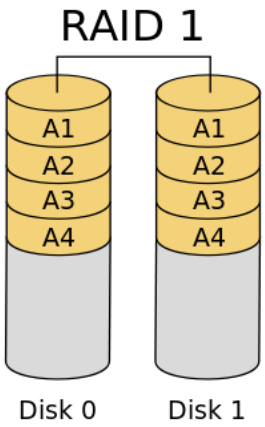


Рис. 2.2. Схема RAID 1

*Достоинства:*

1. Обеспечивает приемлемую скорость записи и выигрыш по скорости чтения при распараллеливании запросов.

2. Имеет высокую надежность – работает до тех пор, пока функционирует хотя бы один диск в массиве. Вероятность выхода из строя сразу двух дисков равна произведению вероятностей отказа каждого диска, т. е. значительно ниже вероятности выхода из строя отдельного диска. На практике при выходе из строя одного из дисков следует срочно принимать меры и вновь восстанавливать избыточность. Для этого с любым уровнем RAID (кроме нулевого) рекомендуют использовать диски горячего резерва.

*Недостаток RAID 1* в том, что по цене двух жестких дисков пользователь фактически получает лишь один.

*RAID 2* зарезервирован для массивов, которые применяют код Хемминга. Массивы такого типа основаны на использовании кода Хемминга. Диски делятся на две группы: для данных и для кодов коррекции ошибок, причем если данные хранятся на $2^n - n - 1$ дисках, то для хранения кодов коррекции необходимо $n$ дисков. Данные распределяются по дискам, предназначенным для хранения информации, так же как и в RAID 0, т. е. они разбиваются на небольшие блоки по числу дисков. Оставшиеся диски хранят коды коррекции ошибок, по которым в случае выхода какого-либо жесткого диска из строя возможно восстановление информации. Метод Хемминга давно применяется в памяти типа ECC и позволяет на лету исправлять однократные и обнаруживать двукратные ошибки.

*Достоинство:* повышение скорости дисковых операций по сравнению с производительностью одного диска.

*Недостаток:* минимальное количество дисков, при котором имеет смысл его использовать, равно 7. При этом нужна структура из почти двойного количества дисков (для $n = 3$ данные будут храниться на четырех дисках), поэтому такой вид массива не получил распространения. Если же дисков около 30–60, то перерасход получается 11–19 %.

*RAID 3* – дисковые массивы с чередованием и выделенным диском четности. Из *n* дисков данные разбиваются на куски размером меньше сектора (разбиваются на байты или блоки) и распределяются по *n* – 1 дискам. Еще один диск используется для хранения блоков четности. В RAID 2 для этой цели применялся *n* – 1 диск, но большая часть информации на контрольных дисках использовалась для коррекции ошибок на лету, в то время как большинство пользователей удовлетворяет простое восстановление информации в случае поломки диска, для чего хватает информации, умещающейся на одном выделенном жестком диске (рис. 2.3) [36].

Отличия RAID 3 от RAID 2: невозможность коррекции ошибок на лету и меньшая избыточность.

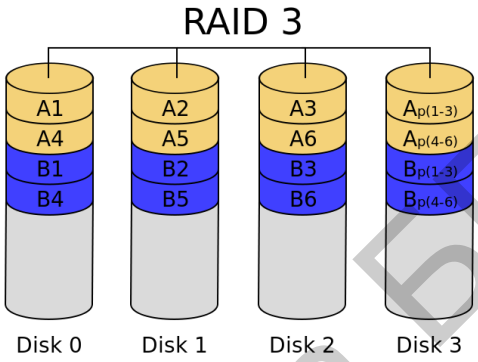


Рис. 2.3. Схема RAID 3

*Достоинства:*

1. Высокая скорость чтения и записи данных;
2. Минимальное количество дисков для создания массива равно трем.

*Недостатки:*

1. Массив этого типа пригоден только для однозадачной работы с большими файлами, так как время доступа к отдельному сектору, разбитому по дискам, равно максимальному из интервалов доступа к секторам каждого из дисков. Для блоков малого размера время доступа намного больше времени чтения.

2. Большая нагрузка на контрольный диск, и, как следствие, его надежность сильно падает по сравнению с дисками, хранящими данные.

*RAID 4* – дисковые массивы с чередованием и выделенным диском четности. RAID 4 похож на RAID 3, но отличается от него тем, что данные разбиваются на блоки, а не на байты. Таким образом, удалось отчасти «победить» проблему низкой скорости передачи данных небольшого объема. Запись же производится медленно из-за того, что четность для блока генерируется при записи и записывается на единственный диск (рис. 2.4) [36].

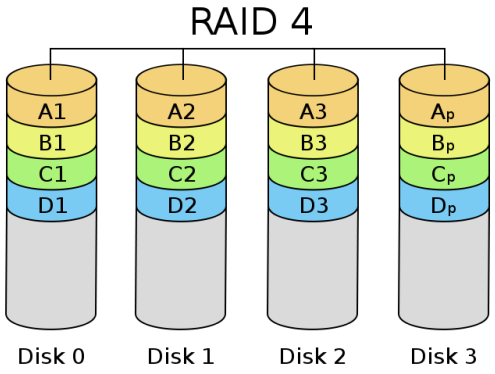


Рис. 2.4. Схема RAID 4

*RAID 5* – дисковый массив с чередованием и «невыделенным диском четности». Основным недостатком уровней RAID от 2-го до 4-го является невозможность производить параллельные операции записи, так как для хранения информации о четности используется отдельный контрольный диск. RAID 5 не имеет этого недостатка. Блоки данных и контрольные суммы циклически записываются на все диски массива, нет асимметричности конфигурации дисков (рис. 2.5) [36]. Под контрольными суммами подразумевается результат операции «исключающее «или». «Исключающее «или» обладает особенностью, которая дает возможность заменить любой операнд результатом и, применив алгоритм «исключающее «или», получить в результате недостающий операнд. Этот метод по сути обеспечивает отказоустойчивость 5-й версии. Для хранения результата операции «исключающее «или» требуется всего один диск, размер которого равен размеру любого другого диска в RAID.

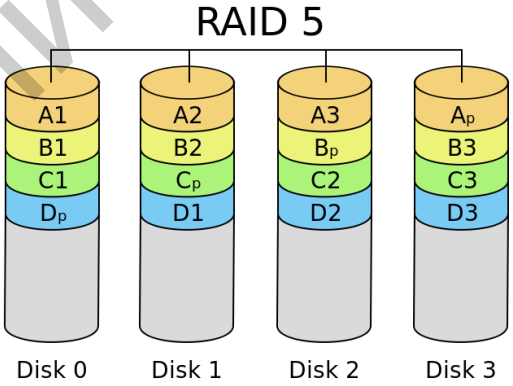


Рис. 2.5. Схема RAID 5

*Достоинство:* экономичность дискового пространства.

*Недостатки:* относительно низкая производительность работы с дисками.

*RAID 6* – дисковый массив с чередованием, использующий две контрольные суммы, вычисляемые двумя независимыми способами. RAID 6 похож на RAID 5, но имеет более высокую степень надежности, под контрольные суммы выделяется емкость двух дисков, рассчитываются две суммы по разным алгоритмам. Требует более мощный RAID-контроллер. Обеспечивает работоспособность после одновременного выхода из строя двух дисков – защита от кратного отказа. Для организации массива требуется минимум четыре диска (рис. 2.6) [36].

Обычно использование RAID-6 вызывает падение производительности дисковой группы примерно на 10–15 %, что вызвано большим объемом обработки данных для контроллера (необходимо рассчитывать вторую контрольную сумму, а также читать и перезаписывать больше дисковых блоков при записи каждого блока).

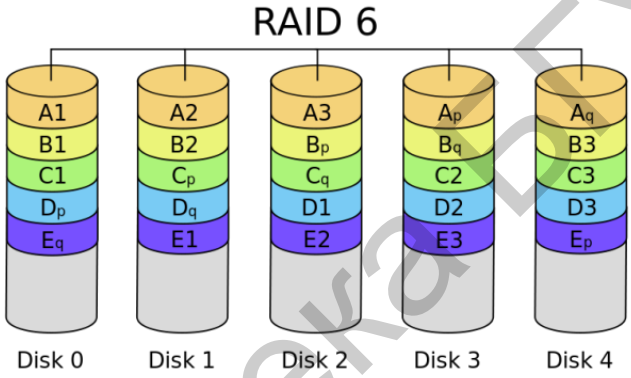


Рис. 2.6. Схема RAID 6

Помимо базовых уровней RAID 0 – RAID 6, существуют комбинированные уровни с названиями вида «RAID α+β» или «RAID αβ», что обычно означает «RAID β, составленный из нескольких RAID α»

## 2.4. Практическая часть

1. Изучить теоретический материал.
2. Исходя из выбранной номенклатуры оборудования по варианту объекта, выданному преподавателем, выполнить расположение оборудования системы безопасности на планах (допускается в случае выполнения проекта систем видеонаблюдения или контроля доступа архитектурную часть изображать условно).
3. Составить спецификацию оборудования и материалов.
4. Оформить отчет о выполнении лабораторной работы.

## 2.5. Контрольные вопросы

1. Назовите основные ТНПА, регламентирующие технические требования к системам охранной сигнализации, видеонаблюдения, контроля доступа, пожарной сигнализации?

2. Поясните понятие основная и вспомогательная части системы безопасности.

3. Расскажите о подсистеме передачи данных: основные требования и характеристики.

4. Расскажите о подсистеме хранения информации: основные требования и характеристики.

5. Расскажите о подсистеме резервирования информации: основные требования и характеристики.

## Лабораторная работа №3. Проектирование линий электропитания и электроснабжение систем безопасности

**Цель:** ознакомление с правилами электроснабжения технических средств противопожарной защиты и выполнение соответствующих расчетов. Выполнение расчета минимального значения сечения кабеля, необходимого для подключения нагрузки.

### 3.1. Электроснабжение средств и систем безопасности

В соответствии с рядом действующих технических нормативно-правовых актов по степени обеспечения надежности электроснабжения электроприемники пожарной автоматики (приемно-контрольные приборы, приборы управления пожарных, функциональных блоков и компонентов установок и систем пожарной сигнализации, пожаротушения, оповещения людей о пожаре, противодымной защиты), как правило, следует относить к I категории надежности.

В данной лабораторной работе рассматриваются основные вопросы по обеспечению электроснабжения технических средств пожарной автоматики по I категории надежности с учетом требований стандарта СТБ 11.16.02-2007 «ССПБ. Устройства электроснабжения технических средств противопожарной защиты. Общие технические условия» (требования аналогичны EN 54–4), действующего на территории Республики Беларусь.

Согласно требованиям указанного стандарта устройства электроснабжения классифицируются следующим образом:

а) по максимальному току нагрузки устройства электроснабжения могут быть малой мощности (до 1,5 А), средней мощности (от 1,5 до 3 А) и большой мощности (более 3 А);

б) по размещению компонентов устройства электроснабжения делятся на внешние (при размещении компонентов в отдельном корпусе от технических средств противопожарной защиты) и встроенные (при размещении компонентов в едином корпусе с техническими средствами пожарной автоматики).

Реализация требования по обеспечению электроприемников пожарной автоматики I категорией надежности выражается в том, что устройства электроснабжения (как внешние, так и внутренние) должны содержать не менее двух источников электропитания: основного и резервного.

При отсутствии по местным условиям возможности осуществления питания электроприемников пожарной автоматики от двух независимых источников допускается осуществлять их питание от разных трансформаторов двухтрансформаторной подстанции или от двух близлежащих однотрансформаторных подстанций, подключенных к разным питающим линиям, про-

ложенным по разным трассам, с устройством автоматического ввода резерва (далее − АВР), как правило, на стороне низкого напряжения [1].

При наличии одного источника электропитания допускается использовать в качестве резервного источника питания электроприемников устройства электроснабжения, соответствующие СТБ 11.16.02 и обеспечивающие бесперебойное питание указанных электроприемников в дежурном режиме в течение 24 ч и в режиме «ТРЕВОГА» – не менее 3 ч (для технических средств оповещения – 1 ч) [1].

При работе устройств электроснабжения от основного источника электропитания (в рабочем режиме) должны обеспечиваться:

а) выходные характеристики (выходное напряжение, номинальный ток, напряжение пульсаций) в соответствии с технической документацией производителя независимо от состояния резервного источника электропитания и его соединительных линий (при выходе из строя аккумуляторной батареи или коротком замыкании соединительных линий работа устройства электроснабжения не должна нарушаться);

б) зарядка аккумуляторной батареи зарядным током требуемой величины (при этом номинальный рабочий ток устройства электроснабжения не должен снижаться в процессе заряда батареи);

в) ограничение или остановка повторной зарядки аккумуляторной батареи при временной пиковой нагрузке (максимальном кратковременном нагрузочном токе, например, при коротком замыкании в линии нагрузки), указываемой в технической документации;

г) контроль работоспособности резервного источника электропитания (для аккумуляторных батарей – контроль при нагрузке с номинальным расчетным сопротивлением с периодичностью 2 ч).

*Примечание.* Для разделения функциональных состояний устройств электроснабжения предусмотрены следующие основные режимы работы:

– режим «Рабочий» – состояние устройства электроснабжения, при котором обеспечивается электроснабжение технических средств пожарной автоматики от основного источника электропитания, а резервный источник находится в исправном состоянии;

– режим «Резерв» – состояние устройства электроснабжения, при котором обеспечивается электроснабжение технических средств пожарной автоматики от резервного источника электропитания;

– режим «Неисправность» – состояние устройства электроснабжения, при котором технические характеристики его компонентов или функции не соответствуют хотя бы одному из требований ТНПА или конструкторской документации [2].

При работе устройств электроснабжения от резервного источника электропитания должны обеспечиваться:

а) выходные характеристики в соответствии с технической документацией независимо от состояния основного источника электропитания и его соединительных линий;

б) электроснабжение технических средств пожарной автоматики при номинальном токе потребления (для аккумуляторных батарей в течение 3 ч) [2].

Таким образом, в качестве основного источника может быть использована общедоступная сеть переменного тока с напряжением 220 В и частотой 50 Гц или источник постоянного тока с напряжением питания от 12 до 110 В. Резервное электропитание может обеспечиваться от второго независимого ввода источника переменного тока или источника постоянного тока (например, аккумуляторных батарей) [2].

При применении в качестве резервного источника электропитания устройств электроснабжения аккумуляторных батарей их емкость определяется расчетом.

Необходимая минимальная емкость $C_{\min}$, А·ч, определяется по формуле

$$C_{\min} = I_{\text{д}} \cdot t_{\text{д}} + I_{\text{т}} \cdot t_{\text{т}}, \tag{3.1}$$

где $t_{\text{д}}$ – время потребления тока в дежурном режиме, ч;

$t_{\text{т}}$ – время потребления тока в тревожном режиме, ч;

$I_{\text{д}}$ – потребляемый ток системой пожарной автоматики в дежурном режиме (при отключении основного источника питания), А;

$I_{\text{т}}$ – потребление тока в тревожном режиме.

Для начала необходимо найти суммарный ток потребления всеми устройствами в цепи в дежурном и тревожном режимах. Расчет суммарного тока потребления всеми устройствами в цепи в дежурном режиме осуществляем по формуле

$$I_{\text{д}} = \sum_{i=1}^{n} I_{\text{д}i} \cdot n_i, \tag{3.2}$$

где $I_{\text{д}i}$ – потребляемый ток $i$-м оборудованием системы пожарной автоматики в дежурном режиме, А;

$n_i$ – количество устройств $i$-го типа.

Расчет суммарного тока потребления всеми устройствами в цепи в тревожном режиме осуществляем по формуле

$$I_{\text{т}} = \sum_{i=1}^{n} I_{\text{т}i} \cdot n_i, \tag{3.3}$$

где $I_{тi}$ – потребляемый ток $i$-м оборудованием системы пожарной автоматики в тревожном режиме, А;

$n_i$ – количество устройств $i$-го типа.

Потребление тока каждым из устройств, входящих в систему в дежурном и тревожном режимах, а также суммарное значение тока в обоих режимах для удобства выполнения расчета могут быть оформлены в виде табл. 3.1.

Таблица 3.1

Потребление тока устройствами пожарной автоматики

| Наименование устройства | Количество | $I_д$, А | $I_т$, А |
|---|---|---|---|
| ... | ... | ... | ... |
| ... | ... | ... | ... |
| ... | ... | ... | ... |
| ... | ... | ... | ... |

При выполнении данного расчета следует помнить, что в соответствии с нормативными требованиями время потребления тока в дежурном режиме составляет 24 ч, а в тревожном режиме − не менее 3 ч (для технических средств оповещения − 1ч ).

*Внимание!* В процессе эксплуатации за счет старения происходит значительное снижение емкости аккумуляторных батарей, поэтому начальную емкость аккумуляторных батарей следует принимать на 25 % больше расчетной.

При выборе устройства электроснабжения следует также обратить внимание на то, чтобы выходной ток источника питания превышал суммарное токопотребление техническими средствами пожарной автоматики как в дежурном, так и в тревожном режимах.

Непосредственный подбор аккумуляторных батарей должен осуществляться на основании выполненного расчета (с учетом 25 % запаса) и выбора источника питания из существующих номинальных значений емкости (у различных производителей количество аккумуляторных батарей в линейке и их номинальные значения могут отличаться).

Устройства электроснабжения (встроенные в корпуса электроприемников или применяемые как отдельное изделие) должны обеспечивать выполнение функций по СТБ 11.16.02.

Устройства электроснабжения и АВР следует размещать децентрализовано у электроприемников. При размещении устройств электроснабжения за пределами помещения, где установлены электроприемники, или на расстоя-

нии более 1 м от электроприемников в пределах указанного помещения, следует предусматривать:

– их соединение с электроприемником по двум линиям электропитания (основной и резервной) с обеспечением бесперебойного электроснабжения при неисправности в одной из линий;

– возможность передачи извещений о неисправности устройства электроснабжения по СТБ 11.16.02 на пожарный пост [1].

Подачу питания к электроприемникам от электросети объекта следует предусматривать от свободной группы щита вводного устройства (при отсутствии свободных групп на указанном щите допускается предусматривать установку для этих целей электрощита на соответствующее количество групп). Щит электропитания, устанавливаемый вне охраняемого помещения, должен размещаться в запираемом металлическом шкафу и быть заблокированным на открывание [1].

### 3.2. Расчет цепей питания системы безопасности

При проектировании систем безопасности важным аспектом является выбор оборудования и кабельной продукции, который влияет не только на качество работы системы, но также и на ее стоимость. Важно знать, а также уметь применять на практике основные расчетные соотношения для определения сечения проводов для слаботочных систем, так как это позволит без затруднений разработать качественную систему с наименьшими финансовыми затратами.

Расчет цепей питания предполагает определение сечения проводов при заданных токах и напряжениях. При расчетах задаются максимально допустимые потери напряжения на проводах, после чего определяется сопротивление проводов и соответственно их сечение. Наибольшую проблему вызывает расчет линии питания с ответвлениями, расположенными на различных участках цепи [1]. Пример такой линии питания приведен на рис. 3.1.

Для этих ответвлений нужно определить напряжение в узлах, необходимое как для расчета сечений проводов между ответвлениями, так и для последующих расчетов линий ответвлений. Трудность обусловлена тем, что между узлами протекают различные токи: на участке $L_1 - I_1 + I_2 + I_3$, на участке $L_2 - I_2 + I_3$, на участке $L_3 - I_3$. Теоретически можно распределить общее падание напряжения между узлами произвольно либо использовать обоснованные пропорции [1].

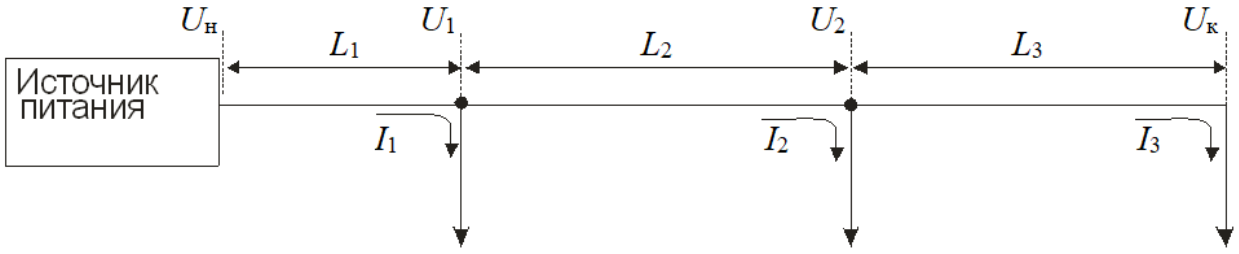


Рис. 3.1. Упрощенная модель линии питания системы оповещения:
$U_н$ – напряжение, выдаваемое источником питания;
$U_к$ – напряжение на последней нагрузке в цепи;
$U_1$, $U_2$, $U_3$ – напряжение в 1, 2, 3 узлах цепи соответственно;
$L_1$, $L_2$, $L_3$ – протяженность 1, 2, 3 участка цепи соответственно;
$I_1$, $I_2$, $I_3$ – ток соответствующей нагрузки

Приведенная методика изложена в упрощенном виде и предназначена для расчета сечений проводов, имеющих промежуточные узлы и ответвления от основной магистрали, а также в предположении, что все провода выполняются с одинаковым сечением.

В основу расчетов положены следующие соотношения:

$$R = \rho(L/S), \tag{3.4}$$

$$U = IR, \tag{3.5}$$

где $R$ – сопротивление провода;

$L$ – длина линии;

$S$ – сечение провода;

$\rho$ – удельное сопротивление провода;

$I$ – ток в линии.

Из выражений (3.4) и (3.5) получаем формулу для нахождения сечения провода:

$$S = \rho LI / U. \tag{3.6}$$

Зная вышеперечисленные соотношения, можно определить ориентировочное значение сечения кабеля без учета влияния расположения нагрузок (например, оповещателей) в разных местах линии и изменения сопротивления материала в зависимости от сечения кабеля. На рис. 2.2 представлен пример линии питания с некоторым конечным количеством нагрузок.

На основании того что падение напряжения представляет собой разность между напряжением, выдаваемым источником питания, и напряжением на последней нагрузке линии, а также учитывая прямой и обратный провод линии системы, получаем следующее выражение для нахождения минимального сечения провода:

$$S = 2\frac{\rho LI}{U_н - U_к}, \quad (3.7)$$

где ρ − удельное сопротивление провода;

$L$ − длина линии;

$U_н$ – напряжение, выдаваемое источником питания;

$U_к$ − напряжение на последней нагрузке в цепи;

$$S = 2\frac{\rho LI}{U_н - U_к},$$

$I$ – ток в линии (в данном случае суммарный ток нагрузки $I = \sum_{i=1}^{n} I_i$ ).

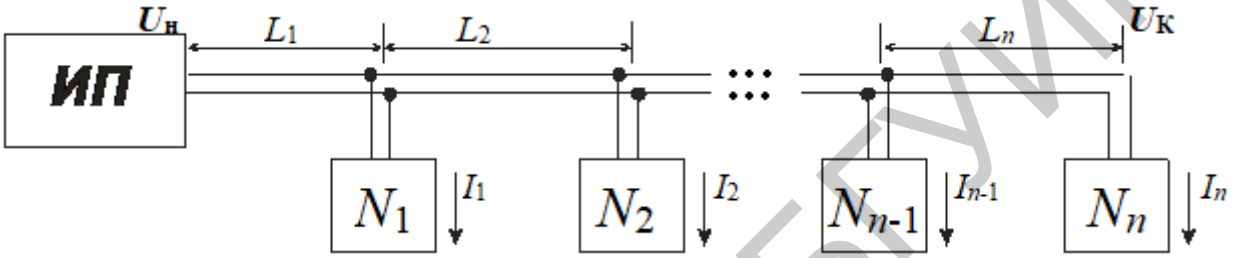


Рис. 3.2. Линия питания системы

При необходимости можно определить сопротивление провода на каждом интервале цепи по формуле

$$R_i = 2 \cdot \rho \cdot (L_i/S), \quad (3.8)$$

где $L_i$ − длина $i$-го участка цепи;

$S$ – сечение провода;

ρ − удельное сопротивление провода.

Отсюда можно вычислить падение напряжения на каждом интервале цепи, используя выражение

$$\Delta U_i = R_i \Sigma I_i, \quad (3.9)$$

где $R_i$ − сопротивление провода на $i$-м интервале;

$\Sigma I_i$ − суммарный ток на $i$-м участке.

Зная падение напряжения на каждом участке линии, можно определить напряжение в любом интересующем узле цепи, начиная с источника питания, с помощью следующего выражения:

$$U_i = U_{i-1} - \Delta U_i, \quad (3.10)$$

где $U_i$ – напряжение в $i$-м узле;

$U_{i-1}$ − напряжение в предыдущем узле;

$\Delta U_i$ − падение напряжения на $i$-м интервале.

Таким образом, зная напряжение в каждом узле, можно поочередно рассчитать линию ответвления от каждого узла. За напряжение источника питания принимается напряжение в узле, за напряжение на конце линии ответвления − минимально допустимое напряжение на нагрузке, установленной в конце цепи, которое определяется технической документацией.

Для того чтобы подобрать необходимую кабельную продукцию при разработке системы оповещения, удобнее оперировать значениями диаметра провода. Зная минимальное сечение провода, диаметр провода можно вычислить, используя следующее соотношение:

$$S = \frac{\pi D^2}{4}, \tag{3.11}$$

где $S$ − сечение провода;

$D$ − диаметр провода.

### 3.3. Практическая часть

1. Изучить теоретический материал.
2. Получить у преподавателя задание.
3. Изучить технические характеристики оборудования, входящего в состав проектируемой системы.
4. Выполнить расчет сечения проводов для системы, указанной в задании, с помощью приведенных расчетных соотношений.
5. Выполнить расчет сечения проводов для системы, указанной в задании, с помощью специального программного обеспечения.
6. Подобрать подходящую кабельную продукцию на основании расчетов.
7. Оформить отчет о выполнении лабораторной работы.

### 3.4. Контрольные вопросы

1. Что собой представляет система резервного электропитания.
2. Опишите модель линии электропитания системы безопасности.
3. Поясните нормативы на время работы систем безопасности от резервного питания.

## Лабораторная работа №4. Проектирование интегрированной системы обеспечения безопасности в местах массового скопления людей

**Цель:** разработка структурной схемы, схемы подключений интегрированной и кабельного журнала системы безопасности.

Рассмотрев основные типы систем обеспечения безопасности, методы их интеграции между собой и сформировав требования к каждой системе, приступим к методам построения комплексной системы обеспечения безопасности на объекте с массовым скоплением людей.

В качестве рассматриваемых систем примем следующие:

1) для систем пожарной автоматики и охранной сигнализации – ИСО «Орион»;

2) для систем контроля и управления доступом – СКУД «Сфинкс»;

3) для систем видеонаблюдения и видеоаналитики – СВН «TRASSIR»;

4) для системы передачи данных – сетевые коммутаторы HP;

5) для системы бесперебойного питания – ИБП Eaton;

6) для системы хранения данных – NAS TRASSIR UltraStorage.

Рассмотрим структуру и состав аппаратного и программного обеспечения в отдельности.

### 4.1. Методические основы построения основных подсистем

**Интегрированная система охраны «Орион»** [37] представляет собой совокупность аппаратных и программных средств для организации систем охранно-пожарной сигнализации, автоматического пожаротушения, а также для создания систем контроля и диспетчеризации объектов. Структурная схема ИСО «Орион» представлена на рис. 4.1 [37].

Система обеспечивает:

– сбор, обработку, передачу, отображение и регистрацию извещений о состоянии шлейфов охранной, тревожной и пожарной сигнализации;

– управление пожарной автоматикой объекта;

– взаимодействие с инженерными системами зданий;

– модульную структуру, позволяющую оптимально оборудовать как малые, так и очень большие распределенные объекты;

– защищенный протокол обмена по каналу связи между приборами.

Задачу системы пожарной сигнализации в составе ИСО «Орион» выполняет адресно-аналоговая подсистема на основе С2000-КДЛ. Подсистема состоит из следующих устройств.

*Контроллер двухпроводной линии связи С2000-КДЛ.*

Контроллер осуществляет централизованный контроль за состоянием пожарных извещателей и обладает возможностью подключения до 127 адресных устройств. В качестве таких устройств применяются адресно-аналоговые извещатели.

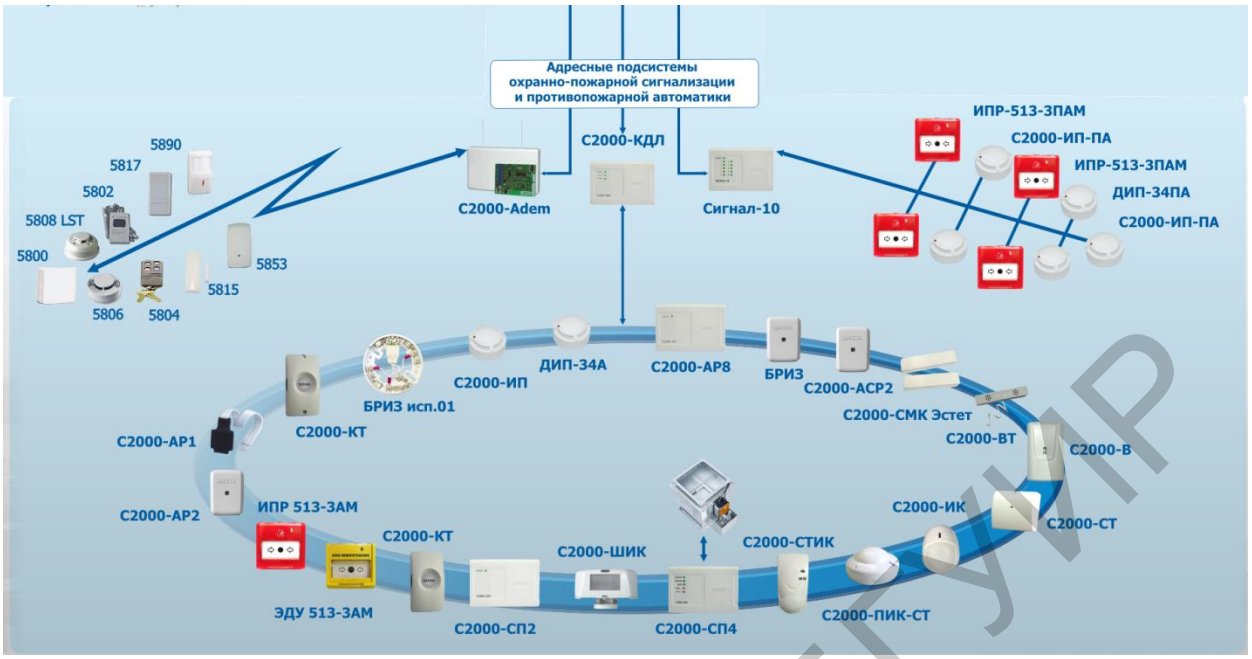


Рис. 4.1. Структурная схема ИСО «Орион»

Для систем пожарной сигнализации применяются:

1. *ДИП-34А-01-02* – извещатель пожарный адресно-аналоговый оптико-электронный предназначен для контроля состояния и обнаружения возгораний, сопровождающихся появлением дыма в закрытых помещениях различных зданий и сооружений, и выдачи извещений «Пожар», «Запыленность», «Внимание», «Неисправность», «Отключен», «Тест».

2. *С2000-ИП-02-02* – извещатель пожарный тепловой адресно-аналоговый максимально-дифференциальный предназначен для контроля состояния и обнаружения возгорания, сопровождающегося выделением тепла, и выдачи извещений «Пожар», «Неисправность», «Тест».

3. *ИПР 513-3АМ исп.02* – предназначен для формирования сообщения «Пожар» при нажатии клавиши.

Для систем охранной сигнализации:

1. *С2000-ИК исп.02* – извещатель охранный объемный оптико-электронный адресный с защитой от животных до 10 кг.

2. *С2000-ИК исп.04* – извещатель охранный поверхностный оптико-электронный адресный. Форма зоны обнаружения типа «штора».

3. *С2000-В* – извещатель предназначен для обнаружения попытки преднамеренного разрушения (взлома) бетонных стен и перекрытий толщиной не менее 0,12 м, кирпичных стен толщиной не менее 0,15 м, деревянных конструкций толщиной материала от 20 до 40 мм, фанеры толщиной не менее 4 мм, конструкций из древесностружечных плит толщиной не менее 15 мм, типовых металлических сейфов, шкафов, дверей и банкоматов.

4. *С2000-СМК, С2000-СМК исп.01, С2000-СМК Эстет* – извещатели охранные магнитоконтактные адресные С2000-СМК и С2000-СМК исп.01 применяются для охраны оконных и дверных проемов (пластиковых и деревянных). С2000-СМК исп.01 имеет провод длиной 1,5 м С2000-СМК Эстет предназначен для охраны металлических дверей и конструкций.

5. *С2000-КТ* – кнопка тревожная предназначена для ручной подачи сигнала тревоги в случае нападения на охраняемый объект.

Для управления системами оповещения, пожаротушения и дымоудаления в ИСО «Орион» применяются следующие устройства:

1. *С2000-СП2 исп.02* – блок сигнально-пусковой адресный С2000-СП2 исп.02 предназначен для работы в составе систем охранно-пожарной сигнализации, оповещения и управления эвакуацией, пожарной автоматики, а также в системах контроля доступа и видеоконтроля.

2. *С2000-СП4* – блок сигнально-пусковой адресный предназначен для управления и контроля клапанов противодымной вентиляции, огнезадерживающих клапанов общеобменной вентиляции, дренчерных клапанов и иных исполнительных устройств. Применяется как часть составного прибора управления в системах пожарно-охранной сигнализации, поддерживающих двухпроводную линию связи, совместно с контролером С2000-КДЛ (версии 2.01 и выше) или С2000-КДЛ-2Ит (версии 1.00 и выше) и пультом контроля и управления С2000М в составе ИСО «Орион».

3. *Рупор исп.01* – прибор речевого оповещения «Рупор» исп.01 предназначен для трансляции предварительно записанной речевой информации о действиях, направленных на обеспечение безопасности при возникновении пожара и других чрезвычайных ситуаций.

4. *Рупор-Диспетчер* – комплекс технических средств обеспечения связи с помещением пожарного поста-диспетчерской Рупор-Диспетчер. Комплекс предназначен для организации связи с диспетчерской с контролем линий связи в системах оповещения и управления эвакуацией (СОУЭ) 4-го и 5-го типов.

Структурная схема системы оповещения и управления эвакуацией представлена на рис. 4.2 [37].

Для управления пожаротушением, как газовым, порошковым, так и водяным и пенным, в ИСО «Орион» предусмотрена серия приборов для контроля исполнительных устройств и сетей системы пожаротушения.

*С2000-ПТ* – блок индикации системы пожаротушения. Предназначен для работы в составе автоматической установки газового, порошкового или аэрозольного пожаротушения. Обеспечивает световую и звуковую индикацию состояния четырех направлений пожаротушения, выполненных на приборах С2000-АСПТ, а также дистанционное управление этими приборами.


Рис. 4.2. Структурная схема системы оповещения и управления эвакуацией

*Поток-3Н* – предназначен для использования в составе ИСО «Орион» для управления оборудованием насосной станции спринклерного, дренчерного, пенного пожаротушения или пожарного водопровода для противопожарной защиты объектов промышленного и гражданского назначения.

*С2000-АСПТ* – предназначен для автономной или централизованной (в составе системы «Орион») противопожарной защиты объектов промышленного и гражданского назначения по одной зоне порошкового, аэрозольного или газового пожаротушения.

Структурная схема системы пожаротушения представлена на рис. 4.3 [37].


Рис. 4.3. Структурная схема системы пожаротушения

Для контроля состояния приборов, управления и настройки системы применяется программное обеспечение *АРМ «Орион Про»*. АРМ «Орион Про» – пакет программного обеспечения для аппаратно-программного комплекса ИСО «Орион», на котором реализуются системы охранной сигнализации, контроля и управления доступом, охранного видеонаблюдения, автоматика противопожарных систем, сопряженные с инженерными системами объектов.

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

АРМ «Орион Про» может функционировать как на одном рабочем месте, так и на распределенных рабочих местах, объединенных через локальную вычислительную сеть. Пакет АРМ «Орион Про» включает в себя программные модули «Сервер», «Администратор базы данных», «Монитор», «Ядро системы», «Оперативная задача», «Генератор отчетов», «Учет рабочего времени», «Видеосервер» и сервисные утилиты. АРМ «Орион Про» способен объединить до 127 локальных ИСО «Орион» одним модулем «Оперативная задача». В составе АРМ «Орион Про» могут одновременно работать до 63 «Оперативных задач». «Оперативные задачи» имеют 6 исполнений – на подключение 4, 10, 20, 127, 512 и 1024 приборов. АРМ «Орион Про» работает с приборами «С2000», «С2000М», «С2000-КС», «Сигнал-20», «Сигнал-20П», «Сигнал-20М», «Сигнал-10», «С2000-4», «С2000-2», «С2000-СП1», «С2000-К», «С2000-КДЛ», «С2000-БИ», «С2000-ИТ», «С2000-АСПТ», «С2000-КПБ», «Рупор», «С2000-ПТ», «Поток-3Н», «С2000-БИ» исп.01, «С2000-КС», «Рупор» исп.01, «С2000-ADEM», «РИП-12-RS», «С2000-Ethernet», «С2000-БКИ», «С2000-ПП», «РИП-12-2А RS», «С2000-BIOAccess-F4», «С2000-BIOAccess-F8», электронный сейф (ключница) «СК-24». Основные показатели системы:

1. Расширенное управление. Более двухсот сетевых клиентов, объединенных в сеть (до 63 «Оперативных задач», до 63 «Мониторов системы», до 63 «Генераторов отчетов», до 15 «Учетов рабочего времени», до 15 «Администраторов базы данных»), 63 сервера обработки видео (до 32 камер на один сервер). Возможность работы со всеми последовательными портами операционной системы, подключение к одному COM-порту до 127 пультов «С2000»/«С2000М», к каждому пульту до 127 приемно-контрольных приборов ИСО «Орион» либо подключение до 127 приемно-контрольных приборов. Подключение системы видеонаблюдения на сетевых IP-камерах «Орион Видео», систем видеонаблюдения и видеорегистрации производства ISS, ITV, VideoNet, Trassir, Vocord, Goal, Ewclid и др.

2. Модульная архитектура и масштабируемость. Система состоит из отдельных функциональных модулей, с помощью которых возможно органи-

зовать полноценное автоматизированное рабочее место на одном компьютере либо создать распределенную сеть рабочих мест, связанных по Ethernet или VPN-каналу. Каждый функциональный модуль за счет гибких настроек обеспечивает возможность специализации отдельно взятого рабочего места под определенную задачу. Наращивание системы реализуется за счет приобретения дополнительных модулей уже и в процессе эксплуатации.

3. Гибкость. Возможность конфигурирования каждого функционального модуля персонально позволяет реализовать конкретную специализацию каждого рабочего места под определенную задачу, программирование сценариев управления с помощью встроенного языка и поддержка наращиваемости определяют способность системы функционировать в соответствии с особенностями и спецификой охраняемого объекта.

4. Надежность – поддержка функционирования локальных рабочих мест с «Оперативной задачей» после потери связи с сервером системы, поддержка горячего резервирования центрального сервера системы. Данный механизм основан на реплицировании базы данных в MS SQL (работает только под управлением MS SQL Server 2008).

**Система контроля и управления доступом «Сфинкс»**. СКУД «Сфинкс» представляет собой совокупность контроллеров «Sphinx» и программного обеспечения для создания систем контроля доступа любой сложности.

*Контроллеры «Sphinx»* предназначены для работы в составе профессиональной СКУД «Сфинкс», производимой российским предприятием «Промавтоматика». Контроллеры «Sphinx» являются сетевыми. Контроллер представляет собой микропроцессорную плату в металлическом корпусе (рис. 4.4) [38].

Автономно поддерживаемые логики работы контроллеров «Sphinx» (не требуют связи контроллера с сервером):

1) графики доступа (временные зоны) любой периодичности от 1 до 31 дня, любое количество интервалов разрешения доступа независимо на вход и на выход;

2) пресечение повторного прохода, зональный контроль;

3) двойная аутентификация: основной признак (бесконтактная карта, отпечаток пальца и т. д.) + PIN;

4) доступ с санкции охраны;

5) доступ в сопровождении (индивидуальная установка групп сопровождения для различных сотрудников);

6) доступ по правилу двух лиц;

7) блокировка доступа через двери, в случае если одна из них открыта (частный случай – организация «шлюза»);

8) автоматическое открытие противоположной двери шлюза после входа в него, немедленно или с программируемой задержкой;

9) ограничение числа лиц в зоне;

10) выдача сигналов управления картоприемником;

11) разблокировка в случае пожарной тревоги;

12) управление статусом блокировки точки прохода двойным поднесением карты сотрудника;

13) управление сторонними контроллерами ворот с помощью программируемой логики (управление непосредственно моторами ворот, выполнение функций контроллера привода).

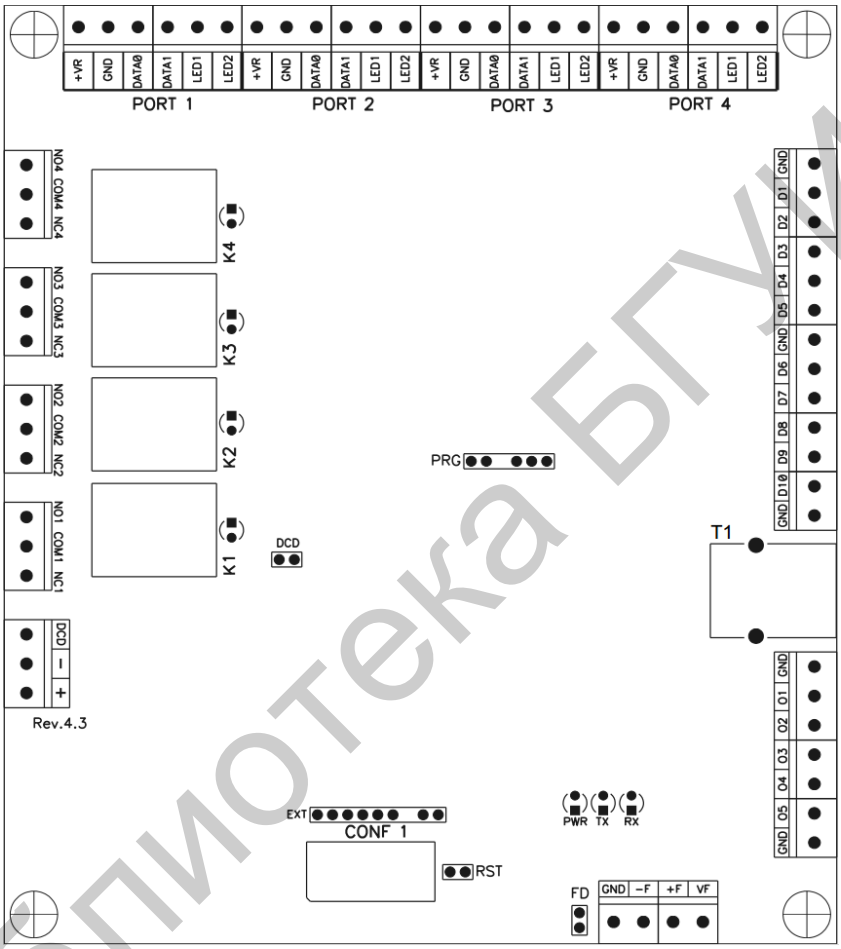


Рис. 4.4. Схема расположения основных элементов на плате контроллеров «Sphinx»

Контроллеры подключаются к сети Ethernet посредством сетевых коммутаторов (рис. 4.5) [38].

*Серверное программное обеспечение СКУД* – часть программного обеспечения системы контроля и управления доступом, обеспечивающая работу сервера (ядра) системы.

К основным функциям серверного ПО СКУД можно отнести:

– создание и поддержание работы сервера СКУД;

– ведение базы данных системы;

– обеспечение возможности подключения клиентских рабочих мест;

– контроль и обработка сигналов от устройств системы по сети;
– обеспечение интеграции с другими системами безопасности.

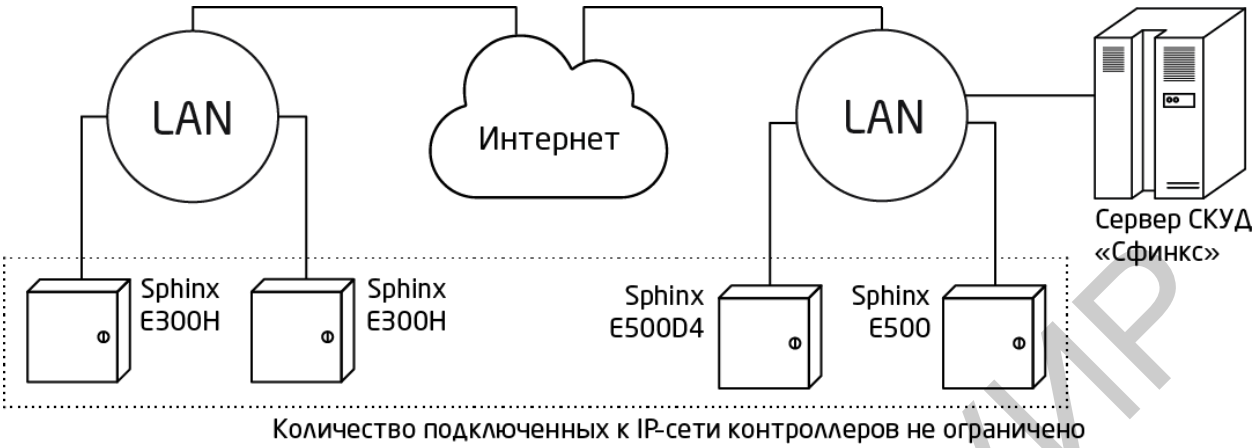


Рис. 4.5. Схема подключения контроллеров Sphinx к сети Ethernet

Клиентское программное обеспечение СКУД – часть программного обеспечения системы контроля и управления доступом, обеспечивающая создание подключения и работу клиентского (удаленного) рабочего места.

К основным функциям клиентского ПО СКУД можно отнести:

– создание подключения к серверу системы;

– обмен и синхронизация информации и событий с сервером системы.

Программное обеспечение СКУД помимо стандартных функций контроля и пресечения проходов имеет также дополнительные. К дополнительным функциям СКУД можно отнести: учет рабочего времени, реакция на события, выдача отчетов, контроль автопарка и другие. В СКУД «Сфинкс» существуют следующие модули [39]:

1) базовый;
2) учет рабочего времени;
3) графическое оформление пропусков;
4) наблюдение и фотоидентификация;
5) интеграция с 1С;
6) расширенная поддержка пропусков посетителей;
7) автопарк;
8) реакция на события;
9) распознавание документов;
10) платежная система;
11) синхронизация данных.

*Базовый модуль* является обязательной частью стандартного программного обеспечения «Сфинкс» [39], а также фундаментом для наращивания функций системы дополнительными модулями. Модуль обеспечивает основные функции СКУД, с его помощью решаются все основные задачи по

настройке системы в целом и контролю статуса ее компонентов. Базовый модуль решает следующие задачи:

– взаимодействие сервера с контроллерами;

– создание учетных записей объектов доступа (рис. 4.6) [39];

– управление режимами доступа (режимы доступа используются системой для принятия решения о возможности прохода объекта доступа относительно направления прохода, времени прохода);

– ведение архива и создание отчетов;

– обеспечение возможности интеграции с другими системами;

– организация рабочих мест (система позволяет создать любое количество одновременно работающих клиентских мест).

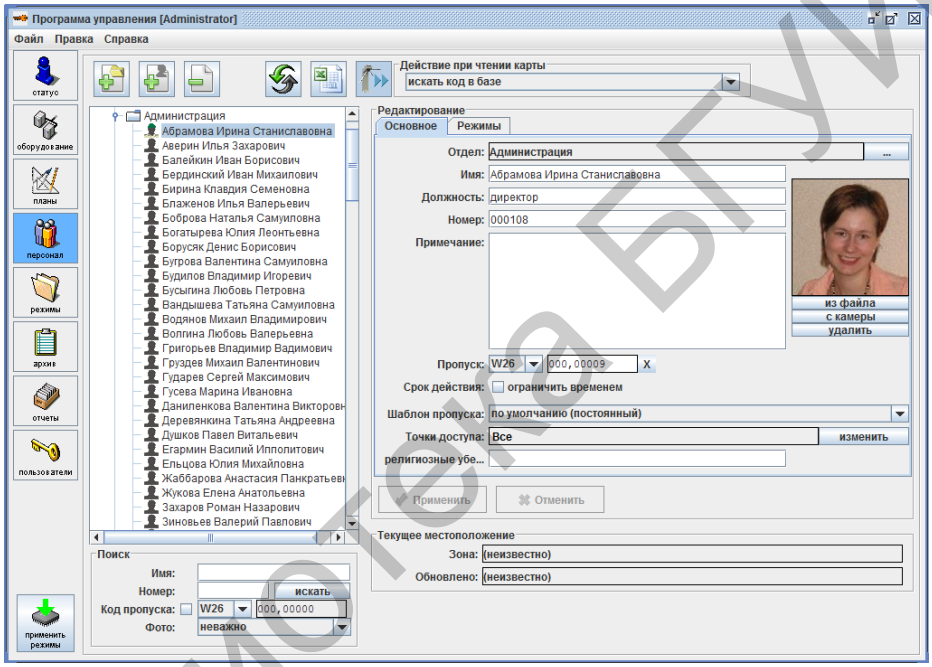


Рис. 4.6. Учетная запись объекта доступа

Автоматизация *учета рабочего времени* упрощает процедуру подготовки отчетности, значительно снижая трудозатраты, а также повышает уровень трудовой дисциплины сотрудников предприятия [39]. Сбор данных о фактических проходах происходит с терминалов «Sphinx E100» или контроллеров «Сфинкс», которые управляют турникетами, дверьми или воротами. Также специально для учета рабочего времени у контроллеров есть режим «Табло регистрации», в котором каждый контроллер поддерживает до двух точек регистрации прихода и ухода сотрудников с помощью любых способов идентификации (бесконтактные карты, биометрика и др.).

*Графическое оформление пропусков.* В системах контроля и управления доступом для идентификации, как правило, используются бесконтактные карты.

Графическая персонализация карты (нанесение информации о владельце, символики компании и т. п.) снижает риск ее подделки, повышает безопасность, а также поднимает имидж организации в целом (рис. 4.7) [39].

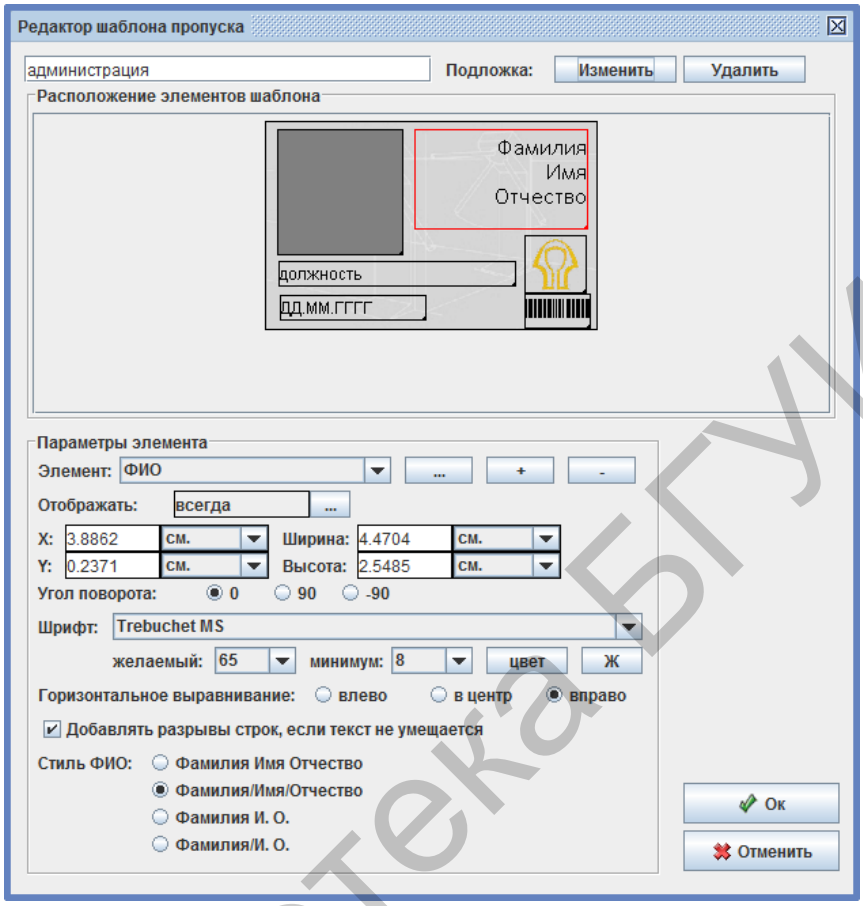


Рис. 4.7. Окно редактора шаблона пропусков

Данный модуль предназначен для графического оформления пропусков сотрудников и посетителей организации. Для каждой из групп сотрудников существует возможность назначения собственного шаблона пропуска.

Для печати пропусков может использоваться как обычный принтер, так и специализированный принтер для печати на пластиковых картах.

*Наблюдение и фотоидентификация*. Этот модуль предназначен для наблюдения за событиями системы в реальном времени (рис. 4.8) [39].

Раскладка окон на экране окна наблюдения может быть изменена на произвольную при помощи редактора (рис. 4.9) [39].

*Интеграция с 1С.* Этот модуль расширяет функции модуля «Учет рабочего времени», добавляя возможность автоматизированно выгрузить табель учета использования рабочего времени (форма Т-13) в «1С:Предприятие».

*Расширенная поддержка пропусков посетителей.* Данный модуль позволяет автоматизировать процессы выдачи (регистрации)/сбора пропусков посетителей.

При регистрации нового посетителя данные документа могут быть введены вручную либо получены в результате работы дополнительного модуля ПО «*Sphinx*» «Распознавание документов» на основании уже имеющегося изображения или изображения, полученного со сканера.

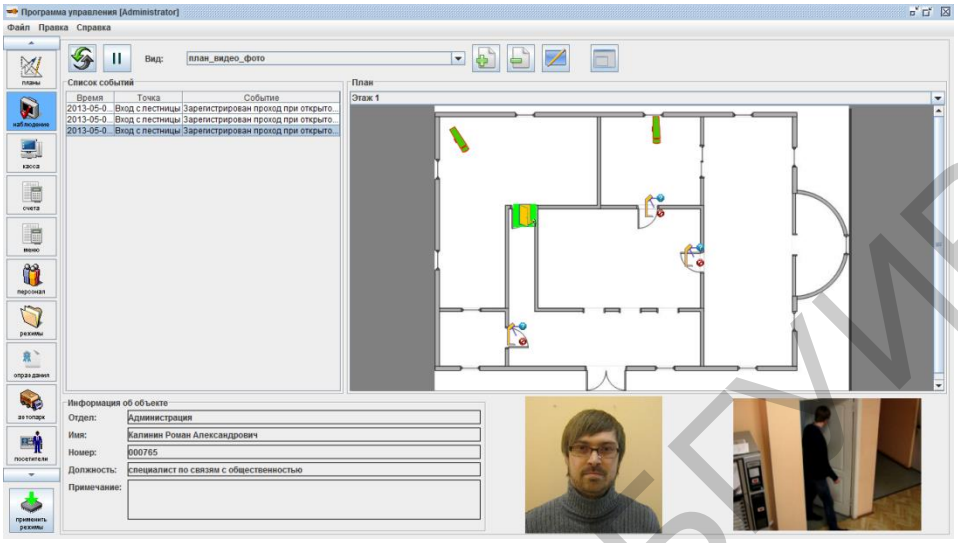


Рис. 4.8. Окно наблюдения

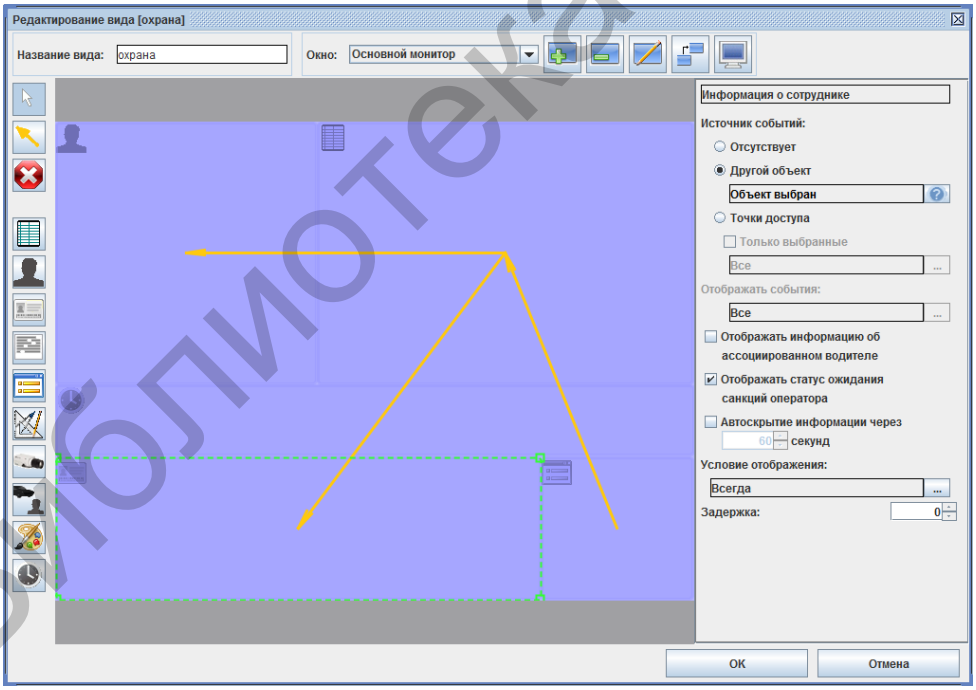


Рис. 4.9. Окно редактора наблюдения

При необходимости имеется возможность добавить фотографию посетителя с веб-камеры (рис. 4.10) [39].

*Автопарк*. Основные функции [39]:

– установление соответствий между сотрудниками и их личным автомобилем (количество соответствий не ограничено);

– создание так называемых «путевых листов» для служебного автотранспорта для установления временного соответствия между сотрудником и служебным транспортом, а также хранение истории их выдачи;

– регистрация перемещения сотрудников на служебном автомобиле.

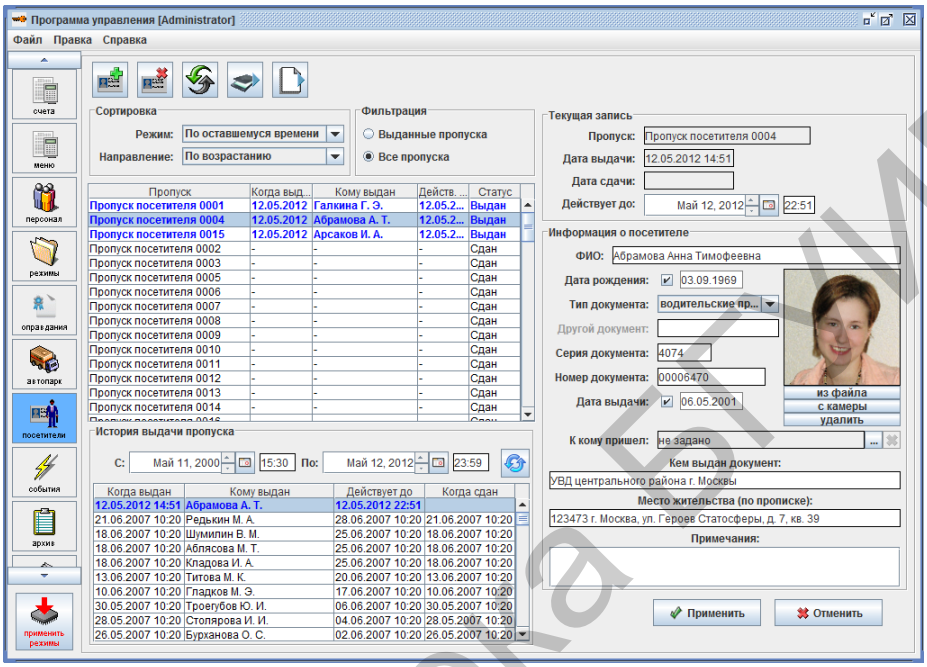


Рис. 4.10. Окно управления посетителями

*Реакция на события.* Данный модуль дает возможность произвольно реагировать на происходящие события, во многом определяет эффективность СКУД и удобство ее использования [39]. Например, благодаря информированию о взломах или выходе из строя точки доступа повышается уровень безопасности на объекте, а возможность смс-уведомлений о проходах конкретных сотрудников позволяет получать максимально оперативную информацию руководству.

Модуль программного обеспечения «Реакция на события» позволяет настроить ответные действия системы, которые будут автоматически выполняться при наступлении каких-либо событий. Количество соответствий «событие – реакция» не ограничено.

Обработка событий, накопленных контроллером в автономном режиме возможна опционально. При отключении этой функции система будет обрабатывать только те события, которые происходят в реальном времени.

При наступлении какого-либо события система осуществляет его обработку и реагирует на него заданным образом.

*Распознавание документов.* Модуль дополнительного программного обеспечения «Распознавание документов» является расширением функцио-

нала модуля «Расширенная поддержка пропусков посетителей»: с его помощью можно осуществлять быстрый ввод данных из паспорта в карточку посетителя, тем самым ускоряя процесс выдачи временных пропусков.

Использование данного модуля подразумевает наличие сканера. Работа может осуществляться как с обычным бытовым сканером, так и специализированным паспортным сканером. В отличие от бытовых сканеров паспортные сканеры имеют большую стоимость, однако компактный размер и высокая скорость сканирования делает их наиболее предпочтительными для оперативной регистрации документов.

Модуль *платежная система* предназначен для организации безналичного расчета за товары и услуги. Типичными вариантами применения функций модуля могут выступать [39]:

– организация питания в корпоративных столовых;

– ограничение числа проходов или продажа проходов через точки доступа (например, в фитнес-клубах, парковках и пр.).

Модуль *синхронизация данных* предназначен для исключения двойного ведения кадровой базы. Данный модуль позволяет СКУД автоматически получать информацию о сотрудниках из уже существующего внешнего источника.

В текущей версии модуля в роли внешнего источника могут выступать:

– любая база данных, работа с которой возможна через стандартный интерфейс ODBC (что справедливо для всех популярных баз данных, включая Oracle и MS SQL);

– 1С:Предприятие;

– Active Directory.

В основе синхронизации лежит последовательное выполнение однотипных циклов синхронизации. В результате работы каждого цикла выявляются и устраняются все отличия данных в БД СКУД «Сфинкс» от данных во внешней системе. Циклы выполняются сервером СКУД «Сфинкс» автоматически с установленной периодичностью.

**Программное обеспечение системы видеонаблюдения TRASSIR** – мощный по функциональности и технологиям софтверный продукт для IP-видеонаблюдения. Это программное обеспечение организует полноценную работу с IP-видеоустройствами производства как DSSL, так и других производителей [40].

В зависимости от мощности используемого видеорегистратора программное обеспечение видеонаблюдения TRASSIR способно записывать до 128 каналов с видеоразрешением 5 Мп (полный кадр) и в реальном времени 25 кадров в секунду каждый канал. Видеорегистраторы с программой видеонаблюдения TRASSIR позволяют одновременно с записью осуществлять просмотр «живого» видео, воспроизведение видео из архива, передачу в сеть большому числу потребителей. Также все другие операции по настройке не прерывают записи. Для записи большого числа каналов программное обеспе-

чение TRASSIR использует фирменную технологию *MultiStor*, равномерно распределяющую записи по всем подключенным дискам. Мало того, данная технология увеличивает надежность сохранения записей при использовании всего объема дисков, так как при выходе из строя одного из дисков будет потеряна только часть информации, в отличие, например, от технологии RAID0 или JBOD. Распределение записи по всем доступным дискам снижает нагрузку на каждый диск в отдельности и не позволяет третировать запись при воспроизведении или копировании данных с какого-либо из дисков.

*Масштабируемость решений.* Один видеорегистратор на базе *TRASSIR* может записывать до 128 каналов видео (5 Мп 25 к/с на канал). Однако это не предел системы, несколько видеорегистраторов TRASSIR могут быть объединены в единый комплекс, так можно построить систему на тысячи каналов.

*Специальные и интеллектуальные функции.* Программа видеонаблюдения TRASSIR может поставляться с дополнительными расширенными возможностями. Распознавание номеров транспортных средств на скорости до 200 км/ч AutoTRASSIR [40] обладает мощным функционалом, не требует настроек и имеет высокую производительность. ActiveDome – наиболее прогрессивная функция управления поворотными камерами SpeedDome [40]. Ускоряет работу оператора в десятки раз, позволяет контролировать множество поворотных камер. В сочетании с SIMT – объектным детектором нового поколения – дает возможность автоматического сопровождения целей скоростными поворотными камерами SpeedDome. DVR, оснащенный детектором SIMT, превращается в мощный инструмент событийного анализа видеозаписей, что совместно с невысокой ценой на программное обеспечение TRASSIR делает систему наиболее мощной на рынке.

*Детектирование движения.* Помимо детекторов движения, встроенных в IP-видеокамеры и IP-видеосерверы, можно использовать другие детекторы, поставляемые с программой видеонаблюдения TRASSIR. GenericDetector, бесплатно поставляемый с системой, имеет детектирование медленного и быстрого движения, выставление произвольных зон детектирования, детектирование лиц в поле зрения видеокамер, детектирование расфокусировки камер, детектирование дыма и открытого огня, детектирование сдвига, ослепления видеокамеры, закрытия ее рукой. Все эти функции создают события в журналах TRASSIR, тревожные сообщения оператору, и по ним в дальнейшем можно осуществлять поиск. Опционально возможно приобретение мощного и многофункционального детектора (детектор видеоаналитики) SIMT, обладающего широкими возможностями по детектированию движения, особенно в уличных условиях [40].

*Ретрансляция видео по сети.* Помимо того что программное обеспечение для IP-видеонаблюдения TRASSIR получает данные с IP-видеокамер и серверов, поддерживается дальнейшая ретрансляция этих потоков. Программное обеспечение обладает следующими возможностями: просмотр жи-

вого видео, видеонаблюдение через Интернет (онлайн), архив, управление настройками.

Программное обеспечение для IP-видеонаблюдения TRASSIR имеет регулируемые ограничения прав доступа к настройкам и функциям. Существует возможность назначения прав пользователям как просмотра определенных камер, так и их настройки, доступа к архивам, сетевым функциям. Количество пользователей с разными правами доступа бесплатно и не ограничено.

В зависимости от мощности видеорегистратора TRASSIR может одновременно воспроизводить 16 и более каналов видео. Поиск видеозаписей может осуществляться как по времени, так и по событиям (CMS). Выбранные фрагменты могут быть скопированы на съемные носители. Поддерживается воспроизведение архива с удаленных устройств.

Запись может быть задана с точностью до минуты для каждой видеокамеры как по детектору движения, так и постоянно. События в DVR могут быть заданы с отсрочкой по времени или исполнению в определенное время.

Детектор саботажа контролирует качество видеосигнала. Автоматическое выявление случаев расфокусировки камеры, изменения ее поля зрения, закрытия объектива или засветки, детектирование обрыва связи с камерой, потери сигнала и пр. Возможность настройки реакции на инцидент, например: привлечение внимания оператора звуковым сигналом и/или сообщением, включение сирены, управление «сухими контактами» и др.

*Возможности интеграции.* Возможность совместной работы системы видеонаблюдения TRASSIR с системами охранно-пожарной сигнализации ИСО «Орион» и контроля доступа «Сфинкс» позволит построить комплексную систему безопасности в одном ПК, управляемую из единого интерфейса. Взаимодействие с интегрированными системами безопасности осуществляется параллельно в едином интерфейсе.

### 4.2. Методические основы построения вспомогательных подсистем

**Коммутаторы для гибких сетей *HP Networking*.** Позволяют строить системы передачи данных любой сложности и распределенности. Архитектура *HP FlexNetwork* [41], основанная на открытых стандартах, подходит для построения надежной корпоративной сети в ЦОД, кампусе и филиалах. Коммутаторы *HP Networking* отличаются высокой производительностью и масштабируемостью. Они оснащены широким набором функций, обеспечивающих хорошую связь центра и периферии, что существенно упрощает и удешевляет сеть.

Требование к коммутаторам определяются самой требовательной системой. Среди систем обеспечения безопасности таковой является система видеонаблюдения. Чаще всего в системах видеонаблюдения применяется PoE-коммутатор *HP 1910-24G-PoE* (рис. 4.11) [41].

Рис. 4.11. Сетевой коммутатор HP 1910-24G-PoE

Устройства серии 1910 [42] предоставляют полный набор возможностей для повышения гибкости. Серия состоит из пяти моделей, монтируемых в стойку, с внутренними блоками питания и трех моделей без поддержки Power over Ethernet (PoE): 8, 24 и 48 разъемов; 2 модели с поддержкой PoE+: 8 разъемов и 24 разъема. Все модели имеют 2 комбинированных разъема восходящей связи.

Эти коммутаторы с интеллектуальным управлением предоставляют интуитивный веб-интерфейс управления. Это гарантия удобства развертывания и управления, а также надлежащего контроля основных функций.

Расширенные средства безопасности, такие как списки управления доступом, IEEE 802.1x и виртуальные ЛВС, защищают сеть от нежелательного или несанкционированного доступа.

Средства управления безопасностью позволяют ограничить доступ к важным параметрам, а также предоставляют несколько уровней привилегий с защитой посредством пароля и поддержку защищенного протокола HTTP (HTTPS).

Коммутаторы серии HP 1910 – это устройства с интеллектуальным управлением, которые обеспечивают расширенные функциональные возможности, включая статическую маршрутизацию уровня 3, порты SFP, поддержку IPv6 и IGMP, ограничение пропускной способности и агрегирование каналов [42].

Коммутаторы этой серии также предоставляют возможности питания IP-устройств посредством PoE+, благодаря чему компании избавляются от необходимости закупки дополнительных электрических розеток.

Передовые технологии производства микросхем позволяют снизить потребление электроэнергии, а ограниченная пожизненная гарантия существенно сокращает общую стоимость владения.

Сетевой коммутатор позволяет подключать как обычный медный кабель «витая пара», так и создавать оптическое подключение.

Программная платформа *HP Intelligent Management Center Enterprise* [45] представляет собой полноценную систему управления проводными и беспроводными сетями, которая поддерживает модель FCAPS (обработка отказов, учет, контроль безопасности и производительности),

обеспечивает возможность комплексного управления ИТ-инфраструктурой, масштабируемость системной архитектуры, а также внедрение новых технологий и решений. Программная платформа Intelligent Management Center (IMC) Enterprise позволяет управлять как устройствами HP, так и решениями сторонних производителей.

Программная платформа HP Intelligent Management Center Enterprise предназначена для предприятий и организаций с филиалами. Она обеспечивает возможности масштабирования от нескольких сотен до нескольких тысяч устройств. Кроме того, она обеспечивает единый центр управления системой обработки отказов, настройки элементов и мониторинга сети.

Программная платформа HP Intelligent Management Center Enterprise обеспечивает возможности управления самыми различными устройствами – от маршрутизаторов и коммутаторов до рабочих станций и серверов. Широкий набор визуальных средств обеспечивает мониторинг устройств, а также предоставляет сведения об устройствах, IP-протоколах, сетевой топологии и т. д. Центр управления безопасности Security Control Center используется для обеспечения единообразия конфигурации устройств. Система оповещений сообщит, если настройки устройства собьются.

Состояние каждого устройства описано на специальной странице со сводной информацией о нем, результатами тестирования подключения и данными, обновляемыми в режиме реального времени. Кроме того, есть возможность установить соединение с устройством по протоколам Telnet/SSH для устранения неполадок.

Центр конфигурации Configuration Center используется для обновления устройств, резервного копирования их данных, а также внесения изменений в настройки. Configuration Center можно также использовать для отслеживания изменений в устройствах.

Программная платформа HP Intelligent Management Center Enterprise предоставляет возможности мониторинга производительности устройств для создания отчетов, просмотра сведений о работоспособности и отправки уведомлений об ошибках.

Решение позволяет устанавливать и отслеживать пороговые значения для отдельных устройств или их групп. При превышении этих значений администратор получает уведомление.

IMC Network Traffic Analyzer включает в себя пять узлов для анализа сетевого трафика и использования сетевых ресурсов различными приложениями и пользователями.

Программная платформа HP Intelligent Management Center Enterprise является одним из первых инструментов управления для интеграции средств администрирования и мониторинга физических и виртуальных сетей.

Решение поддерживает широкий набор гипервизоров, в том числе *VMware vSphere, Microsoft Hyper-V, Citrix Xen и KVM.*

**Система на базе источников бесперебойного питания Eaton** позволяет обеспечивать бесперебойную работу систем обеспечения безопасности в течение требуемого времени [43]. Тип источника бесперебойного питания определяется наличием в системе видеосервера, требования для бесперебойного питания к которому задают тип источника бесперебойного питания с двойным преобразованием. Среди модельного ряда источников бесперебойного питания наиболее часто применяются следующие типы ИБП [43]:

1. Для малых систем обеспечения безопасности: Eaton 5130 UPS. Линейно-интерактивный ИБП Eaton 5130 Rack/Tower подходит для защиты электропитания серверов, систем хранения данных, компонентов VoIP и сетевого оборудования. Этот ИБП обладает размером 2U при мощности до 3 кВ·А. К Eaton 5130 могут быть подключены внешние батарейные модули (EBM) размером 2U, увеличивающие время автономной работы системы. ИБП Eaton 5130 имеет коэффициент мощности 0,9, который позволяет поддерживать большую нагрузку.

2. Для средних систем обеспечения безопасности рекомендуется использовать ИБП Eaton 9SX с двойным преобразованием напряжения с КПД до 95 %, который имеет универсальный корпус с возможностью как вертикальной установки, так и горизонтального монтажа в стойку размером в 19 д.

3. Для крупных систем обеспечения безопасности следует применять ИБП Eaton 9155 с технологией двойного преобразования напряжения, номинальной мощностью 8…30 кВ·А, который обеспечивает надежную защиту электропитания IT-инфраструктур, телекоммуникационного оборудования. Этот ИБП гарантирует максимальный уровень защиты и длительное время автономной работы – и все это в современном компактном дизайне.

Требования по длительности бесперебойной работы определяют также количество дополнительных батарей к ИБП, позволяющих увеличить стандартное время бесперебойного питания.

Каждый ИБП обладает возможностью подключения к сети Ethernet, а также удаленного управления и мониторинга состояния системы бесперебойного питания централизованно. Кроме того, на видеосервер и систему хранения устанавливается программное обеспечение, обеспечивающее безопасное отключение оборудования при истощении аккумуляторных батарей, для предотвращения выхода из строя оборудования из-за резкого обесточивания системы.

**Система хранения данных *TRASSIR UltraStorage*** представляет собой дисковые массивы, разработанные специально для видеорегистраторов повышенной надежности TRASSIR UltraStation для систем видеонаблюдения TRASSIR [44]. Емкость архива систем видеонаблюдения зависит от количества видеокамер, их разрешения, скорости записи, а также требований к сроку хранения архива системы видеонаблюдения. Видеорегистратор TRASSIR UltraStation имеет архив размером от 35 до 180 Тбайт, жесткие диски объемом от 3 до 6 Тбайт с возможностью горячей замены работают в режиме

массива RAID 5. Использование дискового массива TRASSIR UltraStorage позволяет расширить архив дополнительным архивным пространством в 35...114 Тбайт, обеспечив таким образом срок хранения архива до полугода и более.

### 4.3. Оценка эффективности комплексной интегрированной системы обеспечения безопасности

Оценка эффективности систем пожарной сигнализации производится на этапе разработки проектной документации и заключается в расчете требуемых показателей систем пожаротушения и дымоудаления.

Перед выбором системы пожаротушения требуется выполнить расчет пожарной нагрузки [26].

Пожарную нагрузку $P$, МДж/м$^2$, определяют по формуле [26]

$$P = P_n + P_s, \tag{4.1}$$

где $P_n$ – временная пожарная нагрузка (средняя), МДж/м$^2$;

$P_s$ – постоянная пожарная нагрузка (средняя), МДж/м$^2$ .

Во временную пожарную нагрузку включаются вещества и материалы, обращающиеся в производствах, в том числе технологическое и санитарно-техническое оборудование, изоляция, материалы, находящиеся в расходных складах, способные гореть.

В постоянную пожарную нагрузку включаются находящиеся в строительных конструкциях вещества и материалы, способные гореть, за исключением материалов, содержащихся в конструкциях классов К-0 и К-1.

Временную и постоянную пожарные нагрузки определяют по формулам [26]:

$$P_n = \frac{\sum_{i=1}^{j} M_i \cdot H_i}{A}; \tag{4.2}$$

$$P_s = \frac{\sum_{i=1}^{R} M_i \cdot H_i}{A}, \tag{4.3}$$

где $M_i$ – масса $i$-го вещества или материала, кг;

$H_i$ – удельное количество теплоты, выделяемой одним килограммом при сгорании $i$-го вещества или материала, МДж/кг;

$A$ – площадь зданий и сооружений или их частей, м$^2$;

$j$ – число видов веществ и материалов временной пожарной нагрузки;

$R$ – число видов веществ и материалов постоянной пожарной нагрузки.

Так как предпочтительным способом пожаротушения для применения в местах массового скопления людей является тушение мелкодисперсной водой, то следует выполнить расчет водяных установок пожаротушения [26].

Диаметры трубопроводов УП следует определять гидравлическим расчетом, при этом скорость движения воды и раствора пенообразователя в трубопроводах должна приниматься не более 10 м/с.

Гидравлический расчет трубопроводов следует выполнять при условии водоснабжения УП только от основного водопитателя.

Расчетный расход воды, раствора пенообразователя $Q_d$, л/с, через оросительь (генератор) следует определять по формуле [26]

$$Q_d = k\sqrt{H}\ , \tag{4.4}$$

где $k$ – коэффициент производительности оросителя (генератора), принимаемый по эксплуатационным документам на изделие;

$H$ – давление перед оросителем (генератором), м$^{-1}$.

Давление перед оросителем не должно превышать предельных величин (максимальных и минимальных), установленных эксплуатационными документами.

Расход воды раствора пенообразователя необходимо определять произведением нормативной интенсивности орошения $I$, л/(с · м$^2$), на площадь пожара $A$, м$^2$, для расчета расхода воды раствора пенообразователя [26]:

$$Q = I \cdot A. \tag{4.5}$$

Расход воды раствора пенообразователя на внутренний противопожарный водопровод должен суммироваться с расходом ОТВ на спринклерные и дренчерные УП согласно технологическим требованиям.

Эффективность работы системы контроля и управления доступом сильно зависит от типа преграждающих устройств, характера персонала и действующих административных мер на объекте. Стопроцентной эффективности СКУД добиться невозможно, однако есть ряд мер, способных увеличить ее эффективность. Среди таких мер можно выделить:

1. Применение преграждающих устройств на всех возможных входах и выходах объекта. Данная мера увеличит точность СКУД, достоверность информации о местоположении человека и увеличит безопасность.

2. Применение преграждающих устройств высокой эффективности. Эффективность преграждающего устройства зависит от его типа. Наименьшей эффективностью обладают электромагнитные замки, электромеханические замки и защелки, так как доступ по одному идентификатору могут по-

лучить сразу несколько человек, в такой системе отсутствуют элементы разделения потока людей по одному человеку. Следом по эффективности идут шлюзы, ограничивающие количество человек до 2–3, которые одновременно могут пройти на объект по одному идентификатору. Большей эффективностью обладают полуростовые турникеты, у которых данное разделение есть, однако нередки случаи, когда человек проникает на территорию объекта, перепрыгивая или сам турникет или ограждающие элементы вокруг него. Данную проблему способны решить полноростовые турникеты и шлюзы-ротанты, способные максимально эффективно контролировать количество человек внутри и не пропускать, если это количество оказалось более одного.

3. Применение административных мер, при которых сотрудники будут вынуждены регистрироваться при проходе через точку доступа. Такими мерами может быть система штрафов за отсутствие регистрации при проходе через точку доступа либо невыгодное для сотрудника отсутствие события о его проходе через точку доступа.

4. Применение биометрической идентификации. Материальные идентификаторы, такие как бесконтактные карты или брелоки, могут со временем быть утеряны, повреждены или переданы стороннему лицу. Биометрическая идентификация, такая как отпечаток пальца, рисунок вен ладони или сканирование радужки глаза, решает проблему с материальным идентификатором.

Эффективность работы системы видеонаблюдения характеризуется объемом помещения или области, контролируемой видеокамерой с достаточной для распознавания разрешающей способностью. В помещениях такую разрешающую способность достаточно просто получить, применяя камеры с разрешением сенсора в 2...3 Мп и широким (до 90°) углом обзора либо камерами с объективом «рыбий глаз» с углом обзора 180–360°.

В случае видеонаблюдения в уличных условиях для получения максимальной эффективности следует применять поворотные видеокамеры, управляемые компьютером при помощи системы роботизированного управления. В программном обеспечении TRASSIR такой системой является TRASSIR ActiveDome, работающая по принципу определения движущегося объекта в области обзора стационарной камеры и наведения крупным планом поворотной камеры на движущийся объект (рис. 4.12) [46].

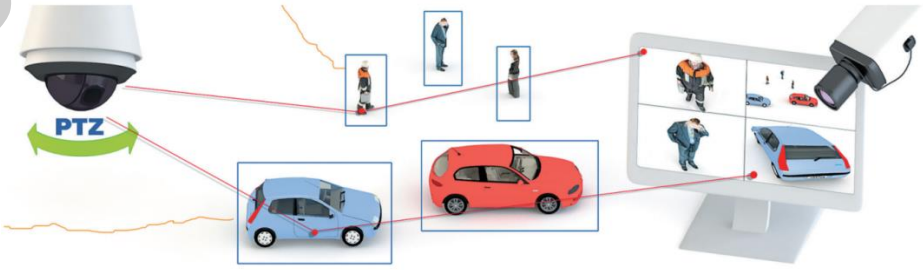


Рис. 4.12. Система роботизированного управления поворотными камерами TRASSIR ActiveDome

Определение эффективности в данном случае осуществляется на стадии проектирования и выбора соответствующего оборудования и определяется площадью, покрываемой областью обзора видеокамеры. При этом важно учесть горизонтальный угол обзора объектива видеокамеры. Расчет угла обзора объектива производится по формуле [47]

$$\boldsymbol{\alpha = 2\mathrm{arctg}\left(\frac{d}{2F}\right)}, \tag{4.6}$$

где α – угол обзора объектива;

$d$ – размер матрицы, мм;

$F$ – фокусное расстояние, мм.

При выборе фокусного расстояния объектива следует учитывать, что угол ясного зрения человека по горизонтали составляет примерно 36°, что соответствует фокусному расстоянию ~ 6,9 мм (для видеокамеры с размером матрицы 1/3»). Поэтому видеокамеры с фокусным расстоянием объектива менее 6,9 мм будут визуально отдалять изображение, более 6,9 мм – соответственно приближать.

## 4.4. Рекомендации по внедрению комплексной системы обеспечения безопасности в местах массового скопления людей

Предположим, что стоит задача оснащения комплексной системой обеспечения безопасности некого крупного объекта с одновременным пребыванием достаточно большого количества человек. Сформулируем основные принципы построения комплексной интегрированной системы обеспечения безопасности.

1. Системы пожарной автоматики.

Для эффективного функционирования систем пожарной автоматики в местах массового скопления людей требуется:

а) применять адресные системы пожарной сигнализации на основе приборов С2000-КДЛ;

б) применять установки пожаротушения тонкодисперсной водой, управляемые через АРМ «Орион Про»;

в) применять установки дымоудаления, обеспечивающие требуемый уровень подпора воздуха, управляемые через АРМ «Орион Про»;

г) применять системы оповещения и управления эвакуацией 4-го и 5-го типов, управляемые через приборы и программное обеспечение АРМ «Орион Про».

2. Системы охранной сигнализации должны обеспечивать полную блокировку всех охраняемых помещений на трех рубежах защиты с применением адресных охранных извещателей в системе ИСО «Орион».

3. Систему ИСО «Орион» при помощи программного обеспечения АРМ «Орион Про» необходимо интегрировать в систему видеонаблюдения TRASSIR.

4. Для осуществления контроля доступа на территорию объекта и в служебные помещения нужно применить СКУД «Сфинкс». При этом следует:

а) в помещениях особой важности установить шлюзы для обеспечения максимального контроля входящих и выходящих лиц;

б) для учета рабочего времени и оплаты труда сотрудников применять полу- и полноростовые турникеты;

в) для доступа на стоянку применять автоматические скоростные шлагбаумы;

г) обеспечивать регистрацию по временным пропускам посетителей служебных помещений с применением картоприемников для сбора временных пропусков;

д) при срабатывании пожарной сигнализации произвести полную разблокировку преграждающих устройств в зоне сработки для обеспечения беспрепятственной эвакуации персонала.

5. СКУД «Сфинкс» необходимо интегрировать в систему видеонаблюдения TRASSIR.

6. Система видеонаблюдения TRASSIR:

а) должна обеспечивать запись изображения по детектору движения, а в особо важных местах – круглосуточно;

б) для обзора за большими площадями применять систему роботизированного управления поворотными видеокамерами ActiveDome;

в) распознавать автомобильные номера въезжающего и выезжающего транспорта;

г) осуществлять подсчет входящих и выходящих в здание людей, иметь возможность вывода информации о проходах за требуемый период времени;

д) управлять системой контроля доступа и охранно-пожарной сигнализации по заданным алгоритмам и правилам.

7. Применять в качестве аппаратной основы видеосервер TRASSIR UltraStation и дисковый массив TRASSIR UltraStorage для обеспечения архива системы видеонаблюдения в течение не менее 60 сут.

8. Применять источники бесперебойного питания Eaton 9155 с дополнительными батарейными модулями Eaton 9155 EBM для осуществления работоспособности комплексной интегрированной системы обеспечения безопасности в течение не менее 2 ч.

9. Применять систему передачи данных на базе сетевых коммутаторов HP.

Система пожарной автоматики ИСО «Орион» в постоянном режиме осуществляет мониторинг ситуации на объекте с применением адресных дымовых или тепловых извещателей. Системы пожаротушения и дымоудаления

работают в дежурном режиме, контролируя исправность линий связи с приборами и выдавая на сервер системы текущую статистику по состоянию каждого устройства. Система интегрирована на программном уровне с системой видеонаблюдения TRASSIR. На экран оператору системы выводится схема объекта с расположенными на них устройствами системы ИСО «Орион», выделяемыми цветовой индикацией состояния (рис. 4.13) [48].

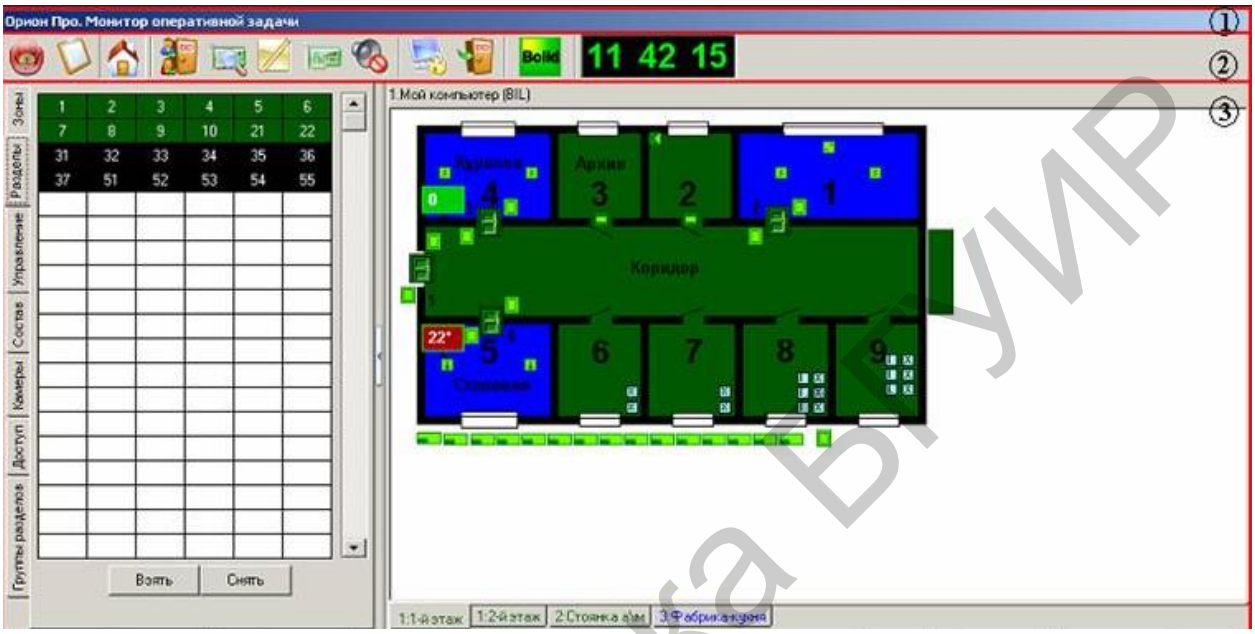


Рис. 4.13. Вид окна мониторинга ПО TRASSIR

Система оповещения и управления эвакуацией в дежурном режиме применяется для служебных оповещений или транслирования музыки и другой информации нетревожного характера. При запуске систем пожарной автоматики система оповещения и управления эвакуацией переходит в тревожный режим оповещения и управления.

К пожарным приборам при помощи аппаратной интеграции подключаются контроллеры СКУД «Сфинкс». При срабатывании системы пожарной сигнализации реле на приемно-контрольном приборе С2000-КДЛ замыкает контакты линии пожарной тревоги на плате контроллера «Sphinx». Точки доступа, управляемые этим контроллером, открываются на свободный проход для осуществления как можно более быстрой эвакуации людей.

В дежурном режиме СКУД осуществляет контроль и управление доступом на территорию объекта и в служебные помещения, выполняет учет рабочего времени, передавая информацию на сервер TRASSIR.

Сервер TRASSIR UltraStation выполняет задачи получения, обработки и хранения данных как от системы видеонаблюдения, так и от других систем комплексной системы обеспечения безопасности. Видеокамеры системы видеонаблюдения размещены во всех помещениях объекта с целью добиться максимальной эффективности системы видеонаблюдения. Видеокамеры под-

ключаются к сетевым коммутаторам HP 1910-24G-PoE, осуществляющим прием сигнала по сети Ethernet и передачу его на сервер. Помимо обмена информацией коммутатор осуществляет питание видеокамер по технологии PoE.

Итоговая структурная схема рассматриваемой системы представлена на рис. 4.14.

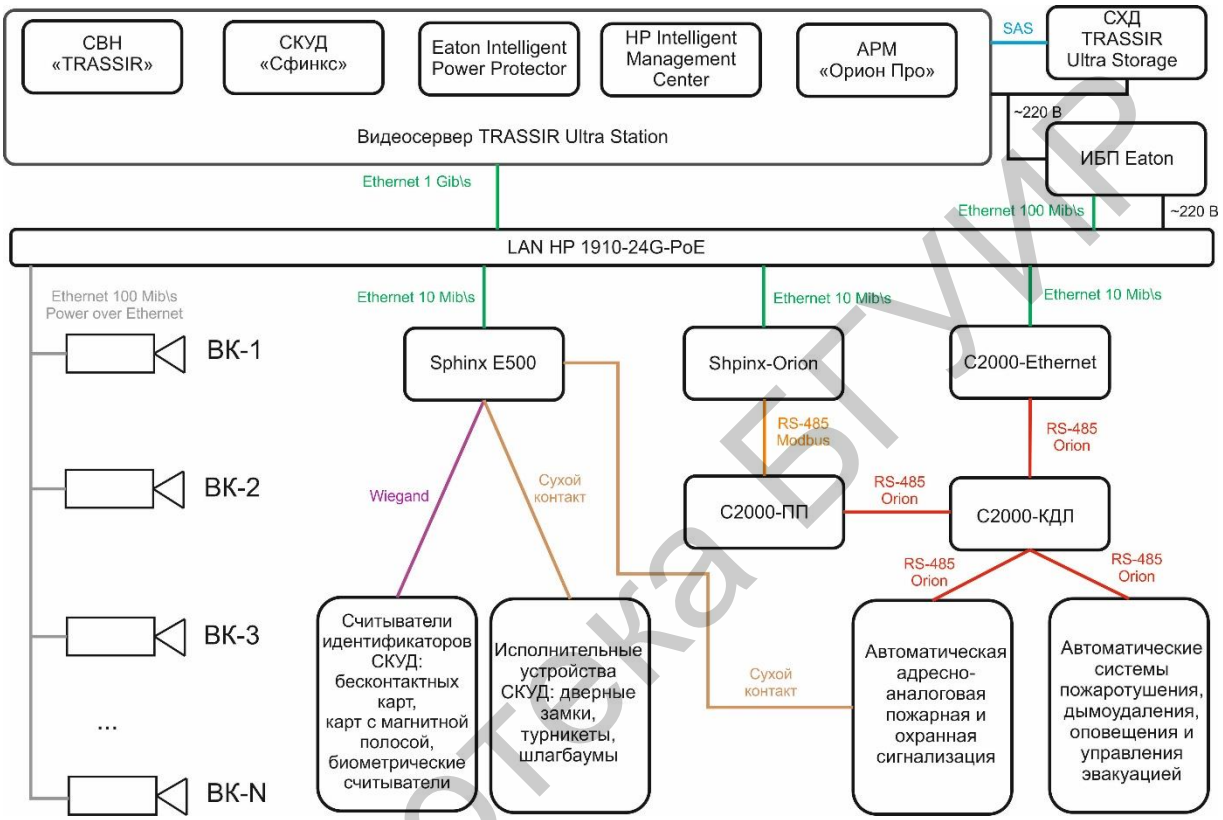


Рис. 4.14. Структурная схема комплексной интегрированной системы обеспечения безопасности в местах массового скопления людей

С целью обеспечения бесперебойного питания системы применяется система бесперебойного питания на базе ИБП Eaton 9155 с дополнительными батареями для осуществления работы системы при отсутствии внешнего питания в течение не менее 120 мин. Указанный ИБП обладает несколькими независимыми защищенными линиями энергоснабжения и осуществляет питание всех элементов системы: видеосервера с системой хранения, сетевого оборудования. Контроллеры СКУД, а также система пожарной автоматики осуществляют питание от собственных источников бесперебойного питания, так как их питающее напряжение составляет 12 В и ИБП на 12 В имеют гораздо меньшую стоимость [49]. На видеосервере установлено программное обеспечение для мониторинга состояния батарей источника бесперебойного питания. При снижении запаса энергии батарей при отключении внешнего

энергоснабжения программное обеспечение осуществляет безопасное отключение видеосервера и дискового массива.

В ПО TRASSIR реализована гибкая система правил и сценариев. Автоматизация позволяет сильно облегчить работу оператора за счет настройки реакций на интересующие и/или тревожные события [50]. Сценарии, в свою очередь, пишут на программном языке Python, позволяющем производить любые действия с системой, как коррекцию поведения системы, так и изменение настроек.

Таким образом, функционирование всей комплексной системы осуществляется из единого программного интерфейса TRASSIR. СВН TRASSIR обладает широкими возможностями автоматизации работы благодаря применению системы правил и сценариев, способных реализовать сценарий реакции на событие любой сложности.

## 4.5. Практическая часть

1. Изучить теоретический материал.
2. По варианту, выданному преподавателем, составить структурную схему, схему подключений интегрированной системы безопасности и оборудования, входящего в нее.
3. Составить кабельный журнал.
4. Подготовить отчет о выполнении лабораторной работы.

## 4.6. Контрольные вопросы

1. Назовите наиболее эффективные основные подсистемы в составе комплексной интегрированной системы обеспечения безопасности в местах массового скопления людей.
2. Назовите наиболее эффективные вспомогательные подсистемы в составе комплексной интегрированной системы обеспечения безопасности в местах массового скопления людей.
3. Опишите систему хранения данных для систем видеонаблюдения TRASSIR UltraStorage.
4. Опишите структурную схему интегрированной системы охраны «Орион».
5. Опишите систему контроля и управления доступом «Сфинкс».

## Список использованных источников


1. Системы безопасности и мониторинга. Интегрированные системы безопасности [Электронный ресурс]. – Режим доступа : http://rovalant.com/systems/integrated-systems.html.

2. Системы безопасности и мониторинга. Система пожарной сигнализации [Электронный ресурс]. – Режим доступа : http://www.rovalant.com/rus/systems/.

3. Промышленные здания и сооружения. Сер. Противопожарная защита и тушение пожаров. В 2 кн. Кн. 2 / В. В. Теребнев [и др.] ; под ред. В. В. Теребнева. – М. : Пожнаука, 2006. – 412 с.

4. Синилов, В. Г. Системы охранной, пожарной и охранно-пожарной сигнализации / В. Г. Синилов. – М. : Академия, 2010. – 512 с.

5. Дымоудаление. Монтаж и техническое обслуживание систем дымоудаления. БелПожПроектМонтаж [Электронный ресурс]. – Режим доступа : http://tc101.by/dymoudalenie.

6. Противопожарная вентиляция. Системы дымоудаления. Инженер.БАЙ [Электронный ресурс]. – Режим доступа : http://ingener.by/info/ventilyaciya/protivopozharnaya_ventilyaciya_sistemy_dymoudaleniya/.

7. Системы пожаротушения. База знаний РОВАЛЭНТ [Электронный ресурс]. – Режим доступа : http://www.rovalant.com/rus/systems/fire-fighting/.

8. Пожарная автоматика. Системы автоматического пожаротушения. ОДО «РеТехГрупп» [Электронный ресурс]. – Режим доступа : http://retech.by/page.php?pg=1&subpg=3.

9. Система охранной сигнализации. База знаний РОВАЛЭНТ [Электронный ресурс]. – Режим доступа : http://www.rovalant.com/rus/systems/burglar-alarm/.

10. Охранная сигнализация. СОБ [Электронный ресурс]. – Режим доступа : http://www.sob.by/safe.php.

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

12. Идентификаторы СКУД. Техническое обеспечение безопасности бизнеса [Электронный ресурс]. – Режим доступа : http://www.e-reading.link/chapter.php/88275/30/Aleshin_-_Tehnicheskoe_obespechenie_beopasnosti_biznesa.html.

13. Исполнительные устройства в СКУД. Каталог статей системы безопасности от А до Я [Электронный ресурс]. – Режим доступа : http://www.sibguardian.info/publ/sistemy_kontrolja_i_upravlenija_dostupom/obshhie_ponjatija_i_rekomendacii/ispolnitelnye_ustrojstva_v_skud/33-1-0-40.

14. Системы охранного телевидения : метод. пособие / Н. В. Будзинский [и др.] ; под ред. Н. В. Будзинского. – М. : НИЦ «Охрана», 2008. – 222 с.

15. Разрешение. Техническое руководство Axis Communications. [Электронный ресурс]. – Режим доступа : http://www.axis.com/ru/products/video/about_networkvideo/resolution.htm.

16. Относительное отверстие. Википедия – свободная энциклопедия. [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki/ Относительное_отверстие.

17. Каталог видеокамер ACTi. ACTi Corporation [Электронный ресурс]. – Режим доступа : http://www.acti.com/products.

18. Термокожух NG-50-135-12. Polyset системы безопасности [Электронный ресурс]. – Режим доступа : http://polyset.ru/ted/% D0%A1%D0%B8%D0%BB%D0%B8%D0%BA%D0%BE%D0%BD_%D1%81%D0%B5%D1%80%D0%B2%D0%B8%D1%81/NG-50-135-12.php.

19. Поворотная видеокамера AC-D6034IR10. Каталог продукции DSSL [Электронный ресурс]. – Режим доступа : http://www.dssl.ru/products/ac-d6034ir10/.

20. Библиотека технических терминов Hikvision [Электронный ресурс]. – Режим доступа : http://hikvision.ru/library.

21. Системы безопасности и мониторинга. Интегрированные системы безопасности [Электронный ресурс]. – Режим доступа : http://rovalant.com/systems/integrated-systems.html.

22. «Хранитель» – медиапортал о безопасности. Тенденции развития программного обеспечения интегрированных систем безопасности [Электронный ресурс]. – Режим доступа : http://www.psj.ru/saver_magazins/detail.php?ID =67135.

23. Интеграция СКУД «Сфинкс» с ИСО «Орион» [Электронный ресурс]. – Режим доступа : http://spnx.ru/int_bolid.php.

24. Перечень ТНПА и их структурных элементов, образующих систему противопожарного нормирования и стандартизации [Электронный ресурс]. – Режим доступа : http://mchs.gov.by/_modules/_cfiles/files/perechen_tnpa_structur.pdf.

25. Технические кодексы установившейся практики и руководящие документы. Департамет охраны МВД Республики Беларусь [Электронный ресурс]. – Режим доступа : http://ohrana.gov.by/legislation/legislation-in-security-activities/.

26. Технический кодекс установившейся практики №45-2.02-190-2010 (02250) «Пожарная автоматика зданий и сооружений. Строительные нормы проектирования» : утв. Министерством архитектуры и строительства Республики Беларусь. – Минск, 2010.

27. Нормы пожарной безопасности №15-2007 «Пожарная автоматика. Область применения» : утв. Министерством по чрезвычайным ситуациям Республики Беларусь. – Минск, 2012.

28. Руководящий документ №28/3.006 – 2005 «Технические средства и системы охраны. Тактика применения технических средств охранной сигна-

лизации» : утв. Министерством внутренних дел Республики Беларусь. – Минск, 2005.

29. Руководящий документ №28/3. 011 – 2001 «Технические средства и системы охраны. Системы контроля и управления доступом. Правила производства и приемки работ» : утв. Министерством внутренних дел Республики Беларусь. – Минск, 2001.

30. Постановление Совета Министров Республики Беларусь от 11 декабря 2012 г. №1135 «Об утверждении Положения о применении систем безопасности и телевизионных систем видеонаблюдения». СОБ [Электронный ресурс]. – Режим доступа : http://www.sob.by/article.php?ID=34.

31. Источники бесперебойного питания. Системы и источники бесперебойного питания СОБ [Электронный ресурс]. – Режим доступа : http://forca.ru/instrukcii-po-ekspluatacii/podstancii/sistemy-i-istochniki-bespereb oynogo-pitaniya-2.html.

32. Олифер, В. Г. Коммутируемые сети Ethernet / В. Г. Олифер // Компьютерные сети. Принципы, технологии, протоколы. – 4-е изд. – СПб. : Питер, 2010. – С. 438.

33. Power over Ethernet. Википедия – свободная энциклопедия [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki/POE.

34. NAS: альтернативная схема хранения данных. Общая информация. Системы хранения данных. Каталог NStor [Электронный ресурс]. – Режим доступа : http://www.nstor.ru/ru/catalog/76/77.html.

35. Дисковый массив. Википедия – свободная энциклопедия [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki/Дисковый_массив.

36. RAID. Википедия – свободная энциклопедия. [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki/RAID.

37. Интегрированная система охраны «ОРИОН» [Электронный ресурс]. – Режим доступа : http://bolid.ru/production/orion/.

38. Система контроля и управления доступом «Сфинкс». Контроллеры «Сфинкс» E500, E900I, R500, R900I. Описание и инструкция по эксплуатации. [Электронный ресурс]. – Режим доступа : http://spnx.ru/dl/Sphinx_E500_E900I_R500_R900I.pdf .

39. СКУД «Сфинкс» – программное обеспечение [Электронный ресурс]. – Режим доступа : http://spnx.ru/soft.php.

40. Программное обеспечение TRASSIR. DSSL [Электронный ресурс]. – Режим доступа : http://www.dssl.ru/products/programmnoe-obespechenie-trassir/.

41. Коммутаторы HP Networking. HP [Электронный ресурс]. – Режим доступа : http://h17007.www1.hp.com/by/ru/networking/products/switches/index.aspx.

42. Коммутатор HP 1910-24G-PoE. HP [Электронный ресурс]. – Режим доступа : http://www8.hp.com/by/ru/products/networking-switches/product-detail.html?oid=4177645.

43. Источники бесперебойного питания Eaton [Электронный ресурс]. – Режим доступа : http://www.eaton.ru/EatonRU/index.htm.

44. Каталог продукции ДССЛ [Электронный ресурс]. – Режим доступа : http://www.dssl.ru/products/.

45. Электронная лицензия на использование программной платформы HP IMC Enterprise, 50-узлов. HP [Электронный ресурс]. – Режим доступа : http://www8.hp.com/by/ru/products/network-management/product-detail.html?oid=5443902#!tab=features.

46. Active Dome – модуль интерактивного управления SpeedDome-камерами. DSSL [Электронный ресурс]. – Режим доступа : http://www.dssl.ru/products/active-dome---modul-robotizirovannogo--upravleniya.

47. Расчет угла обзора видеокамеры – ТехноСфера [Электронный ресурс]. – Режим доступа : http://www.ivtechno.ru/raschet_6.

48. TRASSIR CMS. DSSL [Электронный ресурс]. – Режим доступа : http://www.dssl.ru/products/trassir-cms/.

49. Каталог цен на блоки бесперебойного питания напряжением 12 В. Сфератрейд [Электронный ресурс]. – Режим доступа : http://www.secur.by/rus/catalogue/~group_id__n22=256.

50. Автоматизация TRASSIR. Руководство администратора [Электронный ресурс]. – Режим доступа : http://www.dssl.ru/files/trassir/online_manual_ru/setup-script-folder.html.