МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

Кафедра телевидения и управления
(ТУ)

УТВЕРЖДАЮ
Заведующий кафедрой ТУ, профессор
_____И.Н. Пустынский
«_____»_____2012 г.

ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ

Учебное пособие
для студентов специальностей 080503, 210303, 210312, 100101, 090104, 090106, 090103

РАЗРАБОТАЛ
_____ А.Н. Дементьев
_____ Г.В. Дементьева
«_____»_____2012 г.

2012

Дементьев А.Н., Дементьева Г.В. Технические средства охраны: Учебное пособие. – Томск: кафедра ТУ, ТУСУР, 2012. – 119 с.

В пособии представлены основные положения концепции обеспечения безопасности объектов и личности, даны характеристики средств инженерно-технической защиты, охранной, пожарной сигнализации, видеонаблюдения и систем контроля доступа. Уделено внимание монтажу оборудования. Изложены вопросы организации содержания, технического обслуживания и ремонта технических средств охраны. Представлены основные нормативные документы, регламентирующие проектирование, монтаж и пуско-наладочные работы.

Пособие предназначено для студентов, обучающихся по специальностям 080503, 210303, 210312, 100101, 090104, 090106, 090103.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Проблема обеспечения безопасности становится с каждым годом все более актуальной. В целях повышения уровня безопасности в настоящее время внедряются в практику интегрированные системы обеспечения безопасности, в состав технических средств которых включаются охранная и пожарная сигнализация (ОПС), телевизионные системы наблюдения (ТСН), а также системы управления доступом (СУД).

В системе корпоративной безопасности особое место принадлежит инженерно-техническим методам защиты. Однако у руководителей отдельных фирм, компаний, организаций отношение к их роли колеблется в широком диапазоне от почти полного игнорирования до полной абсолютизации их значения. И тот, и другой вариант не являются оптимальными. С одной стороны, отсутствие инженерно-технических средств защиты существенно ослабляет систему безопасности и требует большой численности службы охраны. Однако с другой стороны, даже излишне дорогой и сложной системе инженерно-технической охраны не удастся полностью избежать использования человеческого фактора. Кроме того, сложные системы для их обслуживания требуют высококвалифицированных, а следовательно, дорогостоящих специалистов. Таким образом, необходим оптимальный баланс между техническими средствами защиты и службой физической охраны.

В предлагаемом пособии делается попытка систематизации материалов о методах организации системы инженерно-технической безопасности фирмы, компании, организации. Этот курс на методологическом уровне взаимодействует с курсами информационной безопасности, теорией корпоративной безопасности, психологией корпоративной безопасности.

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ СИСТЕМНОЙ КОНЦЕПЦИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ

1.1. Исходные положения для разработки системной концепции обеспечения безопасности объектов охраны

Основные направления деятельности по обеспечению безопасности объектов охраны (ОО), привлекательных для преступников с различных точек зрения следующие. Преступные посягательства могут преследовать различные цели, например:

– кражи материальных и/или информационных ценностей;

– имеющие в своей основе террористические действия, направленные на решение политических или грабительских задач, как то: разрушение объекта (вывод его из строя); захват управления функционированием объекта (например, если это объекты радиовещания, телевидения, связи, то захват осуществляется для решения задач дезинформации, пропаганды, информационной блокады населения); информационная разведка; ограбление; внедрение членов организованных преступных формирований (ОФП) или групп (ОПГ) в управленческие структуры и т.д.

Актуальность системного решения проблем и задач охранной деятельности особенно возросла в последние годы, что диктуется многими факторами, например:

– в современных условиях становления новых общественных, экономических, политических, производственных и иных отношений при недостатке механизмов их правового регулирования происходит закономерный взрыв криминогенной обстановки. Резко активизируется деятельность организованных преступных структур, происходит их количественный рост, качественная техническая и методическая оснащенность, проникновение в коммерческие, государственные, в том числе и в правоохранительные органы. По информационно-аналитическим обзорам специалистов (экспертов) уровень преступности в ближайшие годы будет сохраняться;

– преступные действия организованных структур, направленные на захват и ограбление учреждений, на получение конфиденциальной (секретной) информации о деятельности предприятий и т.д., все в большей степени подготавливаются как глубоко продуманные, технически хорошо оснащенные, смоделированные на достаточно высоком интеллектуальном и психологическом уровне акции;

– по данным экспертов подготовка и проведение преступных акций в большинстве случаев осуществляются на высоком профессиональном уровне, характеризуются системным решением (в том числе и в плане сокрытия следов) и часто отличаются жестокостью исполнения.

Исходя из изложенного, разработчики системной концепции обеспечения безопасности объектов в максимальной степени должны учитывать ми-

ровой и отечественный опыт, касающийся всей многогранной деятельности, организуемой по защите объектов.

Практика охранной деятельности показывает, что необходим научно обоснованный подход к решению проблем и задач охраны объектов, в особенности, если это особо важные, особо опасные объекты, объекты особого риска или объекты, содержащие большие материальные ценности (например, банки, хранилища драгоценных камней и металлов и т.д.).

В связи с тем, что наиболее высоким уровнем разработки систем защиты характеризуются особо опасные, особо важные, особо режимные объекты и банки, и этот опыт, безусловно, полезен для объектов многих отраслей народного хозяйства, где возможно придется работать сегодняшним студентам, в списке литературы приведены наименования соответствующих источников, опубликованных в открытой печати.

Очевидно, коль скоро действия преступников часто носят не просто ухищренный, а системно продуманный профессионалами характер, им следует противопоставить организацию и оснащение, выполненные на более высоком уровне профессионализма. Этим и объясняется необходимость разработки обобщенной системной концепции по обеспечению безопасности объектов, которая в каждом случае должна быть адаптирована к конкретному объекту, исходя из условий его функционирования, расположения, характера деятельности, географического положения, особенностей окружающей среды и обстановки и т.д. Таким образом, для каждого конкретного объекта должна разрабатываться на основе общей своя собственная концепция безопасности, исходя из положений которой, разрабатывается проект оснащения объекта инженерно-техническими, специальными и программно-аппаратными средствами защиты.

Технические средства охраны (ТСО), установленные на объектах охраны, должны в комплексе с силами физической охраны и системой инженерных сооружений удовлетворять современным (исходя из сложившейся криминогенной обстановки) требованиям по охране ОО от устремлений потенциального нарушителя.

Учитывая изложенное, разработчики технических средств охранной сигнализации (ТСОС) и комплексов технических средств охраны (КТСО) при анализе исходных положений для определения "моделей нарушителей" должны рассматривать и такие факторы, характерные для современной жизни, как:

– наличие в свободной продаже зарубежных и отечественных изделий спецтехники;

– возможность приобретения современного вооружения;

– возможность рекрутирования организованными преступными формированиями подготовленных в силовых структурах людей;

– наличие значительных финансовых ресурсов в криминальных структурах и т.д., т.е. факторов, расширяющих возможность преступных формирований организовывать против объектов охраны преступные действия с высоким уровнем их предварительной подготовки.

Одной из центральных подсистем в системе обеспечения безопасности ОО является автоматизированная система охраны (АСО), с помощью которой реализуются практические меры по предупреждению недозволенного доступа к технике, оборудованию, материалам, документам и охране их от шпионажа в пользу конкурентов, диверсий, повреждений, хищений и других незаконных или преступных действий.

На практике действия АСО (рис. 1.1) складываются из двух основных фаз: обнаружение нарушителя (в возможно короткий период времени с момента его появления в охраняемой зоне) и его задержание.

Задачи обнаружения нарушителя и определения места его проникновения могут быть решены как с помощью патрулей из личного состава службы охраны, так и с помощью технических средств охраны. Задачи обнаружения нарушителя и контроля за состоянием безопасности охраняемых объектов решаются, главным образом, с помощью технических средств охраны и телевизионного наблюдения. Применение этих средств позволяет в разумных пределах (с точки зрения реализации определенной тактики охраны) снизить численность личного состава охраны, но при этом повысить надежность защиты объекта, увеличить оперативность в принятии мер к задержанию нарушителя.

В общем случае ***в состав комплекса технических средств обеспечения безопасности объекта входят****:* технические средства охранной сигнализации (ТСОС); технические средства наблюдения (ТСН); система контроля доступа (СКД), в литературе применяются также понятия-синонимы – система управления доступом (СУД) и система контроля и управления доступом (СКУД); технические средства пожарной сигнализации (вопросы пожарной безопасности здесь не рассматриваются); технические средства обнаружения диверсионно-террористических средств и технические средства обнаружения (предотвращения) утечки информации. В состав ТСОС входят: средства обнаружения (СО); система сбора, обработки, отображения и документирования информации (ССОИ); вспомогательные устройства (ВУ) – системы электропитания, охранного освещения, оповещения и т.д.

Для решения задач и проблем выбора структуры и состава комплекса технических средств охраны необходимо, во-первых, проанализировать возможные варианты действий злоумышленника. Далее, для определенности, будем применять термин "нарушитель", имея в виду кого угодно, несанкционированным образом проникающего на охраняемую территорию и в его помещения, а именно: случайного, не имеющего определенных целей, человека; вора; грабителя; террориста или группы людей, вторгающихся с преступной целью. Исходя из анализа возможных действий нарушителя, составляются варианты его моделей, которые и принимаются за основополагающий фактор выбора тактики защиты объекта. Во-вторых, более углубленный или менее углубленный учет параметров моделей нарушителей осуществляется, исходя из значимости, ценности, важности объекта, т.е. требуемой категории его защиты (безопасности).

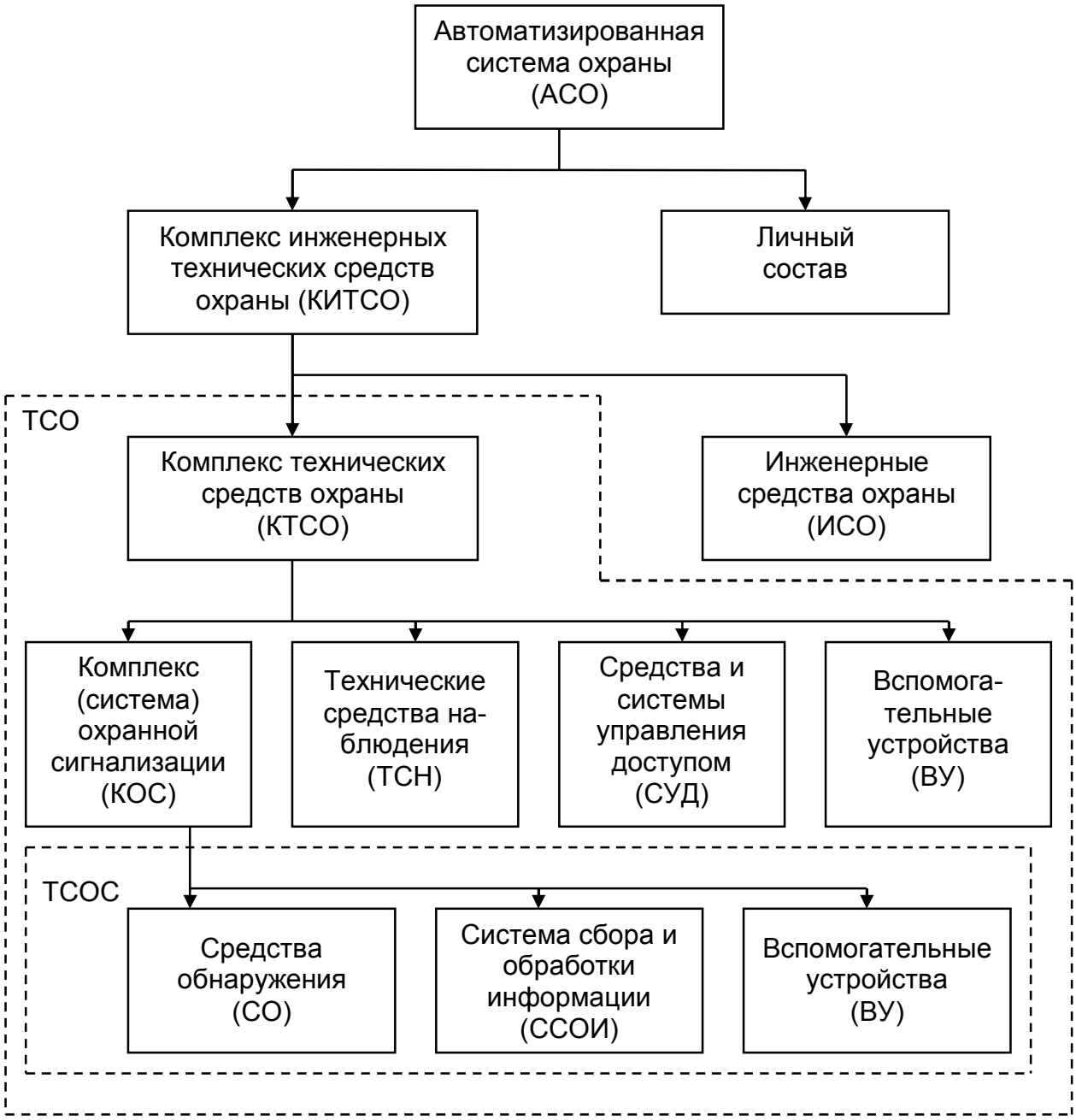

Рис. 1.1 – Структура автоматизированной системы охраны

Важное влияние на оценку параметров нарушителя оказывают его стартовые позиции. Условно их можно разделить на четыре группы:

– нарушитель не имеет доступа на территорию объекта и, соответственно, преодолевает все рубежи охраны;

– нарушитель имеет доступ на объект, но не имеет доступа в режимную зону;

– нарушитель имеет доступ на объект и режимную зону, но не имеет доступа к конкретным охраняемым сведениям или материальным ценностям;

– нарушитель имеет доступ на объект, в режимную зону и к конкретным охраняемым сведениям или материальным ценностям.

Следует отметить, что при более простой (сложной) структуре объекта число стартовых позиций соответственно может уменьшаться (увеличиваться).

Очевидно, что для первой группы вероятность обнаружения и сложность проникновения на объект для совершения противоправных деяний в основном определяется КТСО, а для четвертой -уровнем всей системы обеспечения безопасности, включая и состояние режимной и кадровой работы, проводимой на объекте.

По каждой из возможных угроз необходимо определять территории, подлежащие контролю, и временные интервалы их контроля.

Структурную схему передачи оператору КТСО информации о наличии нарушителя можно представить в виде, приведенном на рис. 1.2.

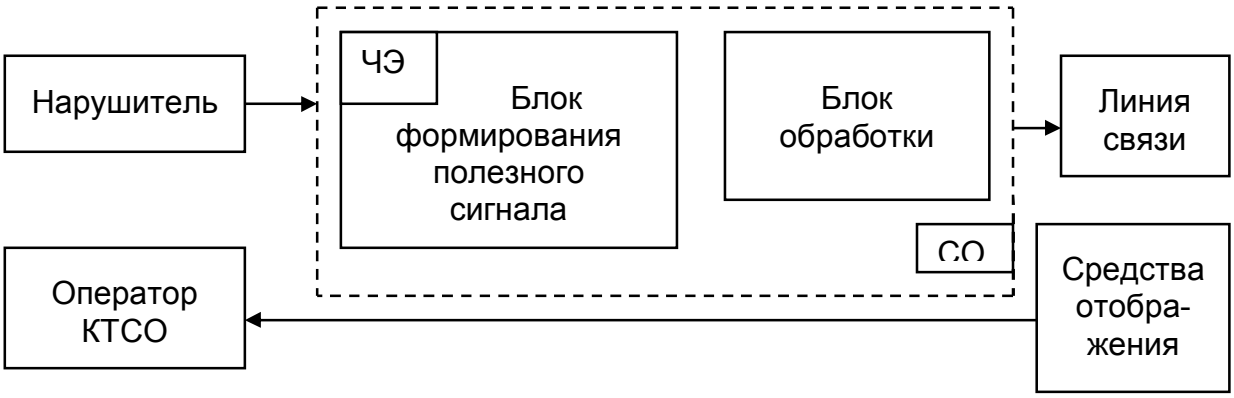

Рис. 1.2 – Структурная схема передачи информации о наличии нарушителя

Наиболее опасным, с точки зрения службы безопасности (охраны) объекта (СБ (О)) является подготовленный и технически оснащенный нарушитель, способный применить для обхода ТСОС множество способов. Очевидно, модель защиты должна строиться, исходя из моделирования всех возможных действий злоумышленника.

Вероятность обезвреживания (обнаружения и задержания) нарушителя силами физической охраны существенно зависит от характеристик ТСОС. Первая фаза – обнаружение нарушителя – определяется вероятностью обнаружения нарушителя ТСОС, периодом наработки на отказ и временем восстановления ТСОС; вторая фаза – задержание нарушителя – зависит от времени обнаружения нарушителя техническими средствами охранной сигнализации с момента его появления на объекте и периода наработки на ложное срабатывание. Последнее объясняется тем, что при ложном срабатывании силы физической охраны отвлекаются на время проверки сигнала "Тревога" и не способны провести проверку двух и более фактов сработки ТСОС одновременно. Кроме того, ложное срабатывание создает с неизбежностью (объективно по законам психологии) стрессовую ситуацию, снижающую боеготовность сотрудников сил физической охраны на некоторый период времени,

необходимый для восстановления гормонального баланса человеческого организма, а также порождает снижение бдительности из-за привыкания к факту появления ложных срабатываний.

Таким образом, при разработке проекта оборудования ОО техническими средствами охранной сигнализации помимо гаммы технических факторов необходимо учитывать факторы, определяемые поведением нарушителя.

Рассмотрим, какие требования к проекту оборудования объекта ТСОС порождаются возможными действиями нарушителя.

Возможность нарушителя найти маршрут, не блокированный СО, должна быть исключена. Для предотвращения прохода нарушителя должны быть блокированы все возможные маршруты движения нарушителя. Состояние физических преград (инженерных сооружений), имеющих большую стойкость и в связи с этим не блокированных СО, должно периодически контролироваться патрулями из личного состава охраны (обходно-дозорной службы) либо – с использованием телевизионных средств наблюдения.

Для увеличения вероятности обнаружения подготовленного и технически оснащенного нарушителя комплексом технических средств охраны объекта могут организовываться полностью скрытные (маскируемые) рубежи охраны.

С целью повышения устойчивости рубежей охраны к преодолению они должны оборудоваться СО, работающими на разных физических принципах действия (радиоволновые, ИК, сейсмические и т.д.), а также должна быть реализована функция дистанционного контроля. Комбинирование данных СО должно производиться по схеме М из N (например, при М=2, N=3, если сработали не менее двух из трех установленных СО, то принимается решение о выдаче сигнала "Тревога"). Числа М и N определяются в ходе проектирования КТСО индивидуально для каждого рубежа охраны объекта.

Для предотвращения обхода нарушителем рубежа охраны путем использования ухищренных способов передвижения необходимо устанавливать несколько СО, как правило, различных физических принципов действия, рассчитанных на блокирование участка при разных способах передвижения нарушителя. Для открытых пространств скорость движения может изменяться от 0,1 до 8 м/с, способы перемещения – от движения "ползком" до движения "в рост"; для физических преград (например, двери и ставни) способами преодоления могут быть открывание и разрушение (полное или частичное). Аналогично рассматриваются способы преодоления замкнутых пространств, а также стен, перекрытий и т.п.

Для предотвращения возможности имитации работы СО нарушителем соединительные линии системы сбора, обработки, отображения и документирования информации (ССОИ) должны иметь физическую и сигнализационную защиту коммутационных шкафов, коробок и т.п. При прокладке кабелей предпочтение следует отдавать скрытой проводке в закладных устройствах (трубах), обеспечивающих дополнительное экранирование и инженерную защиту.

В настоящее время выпускается большое число ССОИ, различающихся числом подключаемых СО, структурой соединительных линий – радиальная (лучевая), шлейфовая (магистральная), древовидная, петлевая (кольцевая) и другими характеристиками. Это позволяет оборудовать объект любого размера наперед заданной группы важности и/или категории защиты. Учет возможности вывода из строя ТСОС подготовленным и технически оснащенным нарушителем проводится при анализе возможных структурных схем построения ТСОС и КТСО в целом. При этом из рассмотрения должны быть исключены варианты, позволяющие замыканием (коротким замыканием) шин питания или информационно-адресных шин КТСО вывести его из строя. Для современных КТСО характерно использование лучевой или древовидной структуры информационно-адресных шин, раздельного управления и автономных защитных цепей электропитания каждого канала.

Ниже рассмотрим некоторые основные требования к выбору аппаратуры ССОИ, определяемые возможностью появления подготовленного и технически оснащенного нарушителя и степенью его подготовки и оснащенности. Возможность обхода ССОИ подготовленным и технически оснащенным нарушителем учитывается при выборе способа передачи информации в ССОИ. Различают три типа аппаратно-программной реализации ССОИ:

I тип – с низкой устойчивостью к обходу;

II тип – со средней устойчивостью к обходу;

III тип – с высокой устойчивостью к обходу.

Под низкой устойчивостью ССОИ к обходу понимают такую организацию опроса СО в АСО, при которой при снятии участка (СО) с охраны состояние соединительной линии и датчика вскрытия СО со стороны АСО не контролируются (отсутствует режим "деблокирование").

Под средней устойчивостью понимают такую организацию опроса СО в АСО, при которой при снятии участка (СО) с охраны состояние соединительной линии и датчика вскрытия СО остаются под контролем АСО (имеется режим "деблокирование").

Под высокой устойчивостью понимают организацию опроса СО, аналогичную средней, но сообщения шифруются с использованием кода, гарантированная стойкость которого к обходу (дешифрации) составляет десятки тысяч часов.

Для предотвращения преодоления ТСО путем оказания воздействия на оператора системы охраны или использования его негативных качеств ССОИ должна иметь режим документирования и иерархическую систему управления, т.е. оператор не должен иметь полного контроля над ССОИ, необходимого лишь при ее настройке, а в системе охраны больших объектов оператор не должен обладать и возможностью снятия (постановки) некоторых участков охраны.

Для того чтобы оперативно обнаружить выход из строя составных частей КТСО, в том числе и в случае преднамеренных действий (саботажа), применяется дистанционный контроль (автоматизированный или автоматический), обеспечивающий проверку работоспособности СО, соединительной

линии и приемной аппаратуры ССОИ, а также повышающий устойчивость ТСОС к обходу соединительных линий и имитации работы СО.

1.2. Системный подход - основа методологии разработки концепции комплексного обеспечения безопасности объектов охраны

Как показали результаты многих исследований, для выработки системного решения, удовлетворяющего необходимым и достаточным условиям обеспечения надежной защиты ОО от подготовленного и технически оснащенного нарушителя, требуется полный учет не только перечисленных выше факторов, но и многих других, как то: состояние инженерных сооружений объекта, состав и уровень подготовки сил физической охраны объекта, окружение объекта, характер объекта (легендируемый, нелегендируемый), расположение и количество сил поддержки, состояние сетей электропитания объекта и т.д.

Многолетний опыт по созданию систем защиты объектов убеждает в безусловной необходимости разрабатывать в каждом случае ***системную концепцию обеспечения безопасности*** конкретного объекта, которая на практике предполагает комплексное взаимоувязанное решение руководством предприятия и службой безопасности (охраны) ряда крупных блоков задач (часть из которых могут решаться лишь с помощью спецслужб при строгом соблюдении соответствующих законов РФ).

1. Определение стратегии комплексной безопасности. Здесь решаются проблемы классификации, систематизации и дифференциации угроз; определяются структура и задачи служб безопасности; разрабатываются (определяются) нормативно-правовые документы, регламентирующие с позиций юриспруденции деятельность служб безопасности (СБ); на основе анализа ресурсов, технико-экономических показателей и социальных аспектов безопасности разрабатываются планы мероприятий по обеспечению безопасности объектов.

2. Обеспечение безопасности от физического проникновения на территорию и в помещения объекта. В этом блоке задач на основе анализа доступности объекта моделируются стратегия и тактика поведения потенциального нарушителя (по всем возможным моделям нарушителей); дифференцируются зоны безопасности; на основе определения ключевых жизненно важных центров объектов разрабатываются принципы и схемы оборудования техническими средствами охранной сигнализации и телевизионного наблюдения, средствами инженерной, технической и специальной защиты рубежей охраны (периметра, территории, зданий, помещений, хранилищ, сейфов, транспортных коммуникаций, средств связи, компьютерных сетей и т.д.). Соответственно, на основе расчета тактико-технических требований выбирается состав и номенклатура технических средств.

3. Защита информации. Решение задач данного блока обеспечивается специальными методами защиты. На основе разработки принципов проверки,

классификации источников информации и каналов ее утечки разрабатываются концептуальные модели защиты от утечки информации, проводятся их оценки на предмет эффективности предлагаемых этими моделями решений. Здесь решается широкая гамма задач разработки методов защиты по всем возможным каналам утечки (речевой, визуальный, виброакустический, электромагнитный, проводной, за счет паразитных связей и наводок и др.). Разрабатывается нормативная база по защите от утечки информации. На основе моделирования возможных способов приема информации потенциальным нарушителем за пределами помещений посредством применения направленных микрофонов, лазерных средств и т.п. вырабатываются методы пассивной и активной защиты.

4. Защита от прогнозируемых к применению средств вне-гласного контроля. Эти задачи ориентированы на модель нарушителя – сотрудника учреждения, либо на проведение контрразведывательных мероприятий, если по оперативным каналам получена информация о заинтересованности, которую проявили организованные преступные формирования к данному объекту. Здесь решается ряд специфических задач от выбора и установки средств негласного контроля до выбора организационно-режимных мер защиты от негласного контроля со стороны потенциального нарушителя. Большое внимание здесь уделяется техническим средствам дефектоскопии, автоматизации средств контроля трактов передачи информации, анализу системы демаскирующих признаков и ряду других[1].

5. Защита от диверсионно-террористических средств (ДТС). Задачи данной предметной области также решаются специальными методами защиты. На основе исследования, классификации и моделирования вариантов активных действий террористов, прогнозирования возможных способов доставки ДТС на территорию объекта, изучения каналов управления диверсиями и технических способов их осуществления (например, с использованием радио взрывателей) выбирается аппаратура обнаружения ДТС, разрабатываются организационно-технические мероприятия по созданию контрольных пунктов, постов проверки, использованию меточной техники и ряд других. Разрабатываются рекомендации по выбору техники обнаружения.

6. Обеспечение безопасности (защита информации) в локальных вычислительных сетях (ЛВС) и ПЭВМ, т.е. в автоматизированных системах обработки информации (АСОИ). Здесь на основе анализа моделей нарушителей, классификации видов угроз и видов компрометации информации разрабатывается комплексный подход к защите информации в автоматизированных информационных системах, ЛВС, серверах и ПЭВМ, соответствующая нормативно-правовая база защиты, регламентирующие документы; раз-

---

[1] Эти и схожие задачи, излагаемые в тексте книги, решаются строго в рамках:

1. Федерального закона Российской Федерации об оперативно-розыскной деятельности (№144-ф3 от 12.08.1995 г. с учетом редакций от 18.07.1997 г., №101-ф3; от 21.07.1998 г., №117-ф3; от 5.01.1999 г., №6-ф3; от 30.12.1999 г., №225-ф3 и от 20.03.2001 г., №26-ф3).
2. Уголовно-процессуального кодекса Российской Федерации (вступившего в силу с 1.07.2002 г., основные статьи применительно к предмету учебного пособия – №№165; 168).

рабатываются методы и способы программно-аппаратной защиты от несанкционированного доступа и копирования (НСД, НСК). Особое место занимают разработка и внедрение специальных математических и программных методов защиты операционных систем, баз данных и серверов, методов идентификации пользователей и ЭВМ, паролей, ключей и антивирусных программ. На основе определения и анализа задач СБ разрабатываются организационные меры защиты.

7. Защита систем связи. С точки зрения проведения разведывательных операций со стороны ОПФ (Г) необходимость тщательной разработки данного блока задач является чрезвычайно актуальной, ибо наиболее доступными для перехвата нарушителем информации, безусловно, являются каналы связи.

Здесь на основе классификации сетей связи разрабатываются методы оптимизации связи, криптографической защиты, защиты телефонных сетей связи. Наряду с решением проблем стандартизации защиты, создаются специальные методы и способы, обеспечивающие конфиденциальную связь.

8. Человеческий фактор в системе обеспечения безопасности. Здесь рассматривается блок задач, решаемый детективной группой службы безопасности, как-то:

- разработка и реализация мероприятий по изучению лиц из числа персонала и иных лиц, в действиях которых содержатся угрозы безопасности деятельности учреждения посредством воздействия на его сотрудников, их близких и родственников;
- проверка кандидатов для приема на работу;
- разработка и реализация мероприятий по обеспечению "чистоты рук";
- организация взаимодействия и поддержание контактов с силами поддержки и/или правоохранительными органами по вопросам обеспечения безопасности и многое другое.

9. Исследование средств отечественного и зарубежного вооружения, которые могут применяться для поражения объектов. В данном блоке задач должны быть рассмотрены возможные способы и применяемые организованными преступными формированиями (или исполнителями – одиночками) виды вооружения, взрывчатых или иных поражающих веществ для осуществления вооруженной акции.

Здесь на основе анализа тактико-технических характеристик традиционных и нетрадиционных средств поражения объектов должна быть дана классификация этих средств, описаны характерные признаки их поражающего действия, методы и способы их обнаружения, локализации, обезвреживания или уничтожения, а также проведена оценка эффективности систем охраны и обороны объектов.

10. Организация системы контроля доступа. Этот блок задач направлен на эффективную реализацию процедур проверки человека, пытающегося открыто ("законным образом") проникнуть на территорию объекта, в отдельные его помещения и режимные зоны. Здесь решаются задачи идентифика-

ции – это установление тождества (опознание личности) по совокупности общих и частных признаков и аутентификации – это установление подлинности личности.

Кроме десяти перечисленных (напрямую связанных с оперативной охранной деятельностью) существуют иные блоки задач, рассматривающих как общесистемные проблемы, например, определение приоритетов (иерархий) во взаимодействии элементов системы безопасности, так и специальные, например обеспечение пожарной безопасности. Области охранной деятельности, связанные с реализацией названных задач, чрезвычайно многогранны.

Взаимоувязанное решение перечисленных блоков задач ***системной концепции обеспечения безопасности объекта,*** в каждом из которых существуют свои подходы, методы и способы решения, должно обеспечить непротиворечивость и полноту принимаемых мер защиты. Только в этом случае можно говорить о выполнении ***необходимых и достаточных условий*** в деле защиты объекта от подготовленных и технически оснащенных нарушителей.

Реализация каждого из блоков задач осуществляется посредством разработки проекта, который носит индивидуальный для учреждения и объекта (территории, здания, этажа, помещения) характер. В зависимости от категории важности объекта этот проект должен обладать соответствующими грифами секретности. Однако и для нережимных объектов охраны такой проект должен носить строго конфиденциальный характер, т.е. быть доступным строго ограниченному кругу лиц из числа сотрудников СБ(О) и руководства.

Необходимость комплексного решения (на основе системного подхода) перечисленных основных (типовых) блоков задач проистекает из того, что профессионализму ОПФ (Г), безусловно, следует противопоставить организацию и оснащение, выполненные на более высоком уровне профессионализма. Однако, коль скоро абсолютной защищенности быть не может, в каждом случае проводятся сравнительные оценки затрат на защиту и возможные потери при сознательном отказе от применения несоизмеримо дорогостоящих (относительно потерь) методов и технических средств защиты.

В мировой практике уже давно используется такое понятие как система защиты, под которой подразумевается комплекс организационных и технических мероприятий, направленных на выявление и противодействие различным видам угроз деятельности объекта. Рассмотрение возможных угроз проводится по следующим основным направлениям:

– безопасность персонала: неэффективная защита может привести к ущербу здоровью или даже угрозе жизни сотрудников;
– угрозы материальным ценностям, имуществу и оборудованию;
– безопасность информации.

Существенным при оценке угроз и выборе приоритетов в системе защиты является учет международного опыта по организации охранной деятельности применительно к объектам конкретного вида, например, банков, предприятий, крупных офисов и т.д. Этот опыт берется за основу и при подготовке современных нормативов защиты. Так, например, западно-европейские фирмы – производители оборудования для систем банковской защиты при-

держиваются единых критериев оценки угроз, согласно которым для сейфовых комнат – хранилищ ценностей и компьютерной информации приоритеты направлений защиты следующие:

– терроризм, стихийные бедствия и аварии, пожары, наводнения, механическое разрушение;

– несанкционированный (неразрешенный) съем информации из компьютерного банка данных;

– несанкционированное проникновение в сейфовую комнату как с целью кражи ценностей, так и с целью кражи информации.

Несмотря на существенные различия в природе угроз, создание защиты от каждой из них должно идти в комплексе со всей системой. Например, несанкционированный съем информации может осуществляться дистанционно путем контроля из соседнего здания излучений от средств обработки банка данных, в котором может содержаться информация конфиденциального характера. Защитой от такого вида угрозы является экранирование аппаратуры и коммуникаций, применение специальной аппаратуры, искажающей картину электромагнитного поля излучения. Но съем информации можно проводить и с помощью специально внедренных в помещение подслушивающих устройств, как то: микрофоны, радиозакладки и т.п. (см. примечание выше). Защитой в этом случае будет поиск техники подслушивания с привлечением компетентных органов, а также строгое соблюдение режима доступа в помещение или в здание, что является защитой и от несанкционированного проникновения.

В основе разработки системы защиты объекта и организации ее функционирования лежит принцип создания последовательных рубежей, в которых угрозы должны быть своевременно обнаружены, а их распространению будут препятствовать надежные преграды. Такие рубежи (зоны безопасности) должны располагаться последовательно от ограждения вокруг территории объекта до главного особо важного помещения, такого как хранилище материальных и информационных ценностей.

Защита объекта должна состоять из различного рода ограждений его периметра и специально оборудованных въездов и проходов, решеток на окнах и в дверных проемах, резервных выходов из здания, охранной сигнализации, охранного освещения и охранного теленаблюдения.

Элементы защиты всех участков объекта должны взаимодополнять друг друга. Эффективность всей системы защиты от несанкционированного проникновения будет оцениваться по максимуму времени, которое злоумышленник затратит на преодоление всех зон безопасности. За это же время должна сработать сигнализация, сотрудники охраны установят причину тревоги, примут меры к задержанию злоумышленника и вызовут подкрепление из ближайшего отделения милиции или из сил поддержки.

Таким образом, эффективность системы защиты оценивается величиной времени с момента возникновения угрозы до начала противодействия или ликвидации ее. Чем более сложная и разветвленная система защиты, тем

больше времени потребуется на ее преодоление и тем больше вероятность того, что угроза будет своевременно обнаружена, определена и отражена.

Современные системы безопасности основываются на реализации комплекса мероприятий по организации физической, инженерной, технической и специальной защиты.

В общем виде укрупненная структурная схема системы обеспечения безопасности объекта представлена на рис. 1.3.

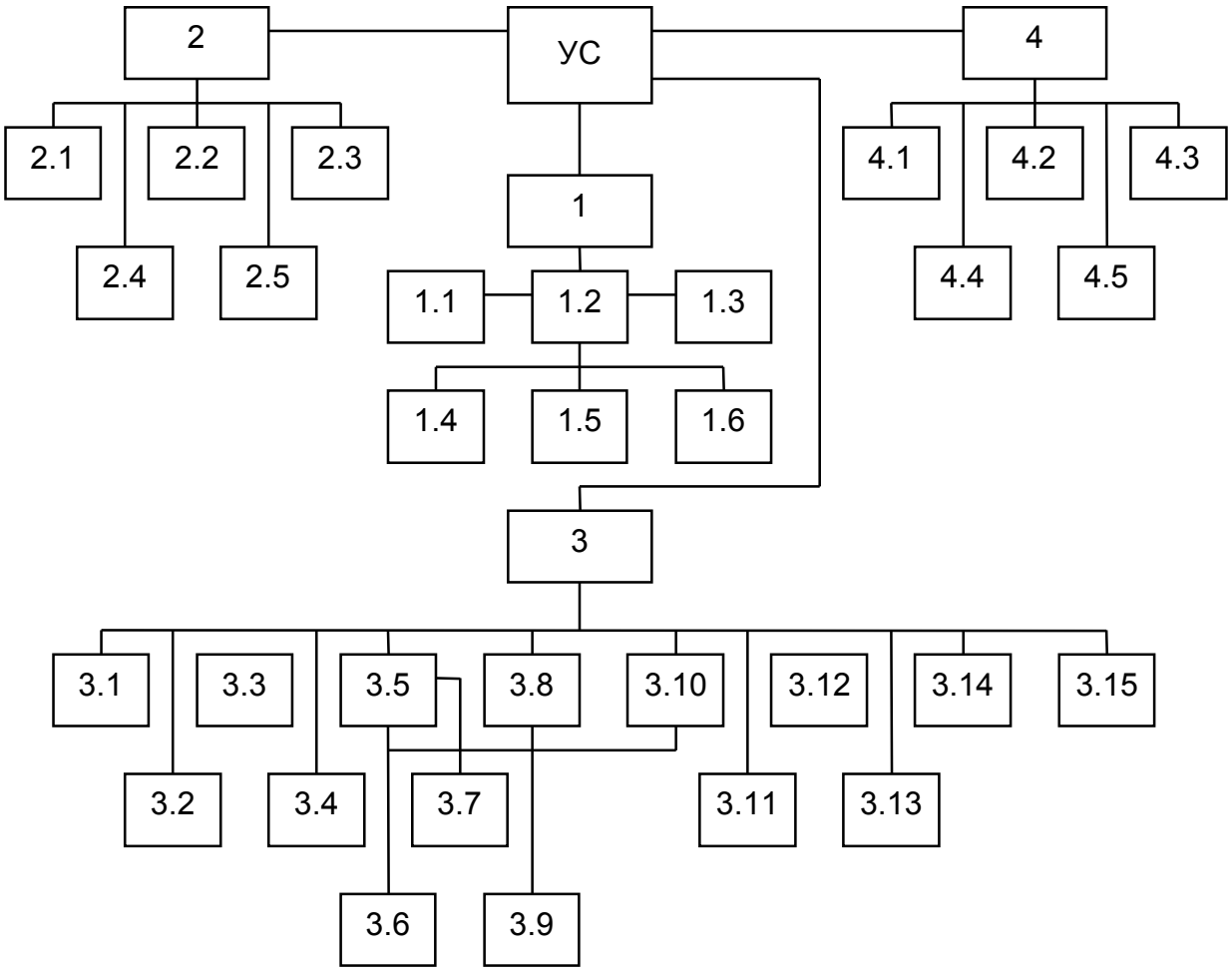

Рис. 1.3 – Укрупненная структурная схема системы обеспечения безопасности объекта

На рис. 1.3 приняты следующие обозначения:

УС – укрупненная структурная схема системы обеспечения безопасности объекта

1 – физическая защита

1.1 – объектовая и/или городская пожарная команда

1.2 – служба охраны

1.3 – наряд милиции и/или силы поддержки

1.4 – работники контрольно-пропускного поста

1.5 – операторы технических средств охраны

1.6 – тревожная группа и подвижные посты

2 – инженерная защита
2.1- усиленные ограждающие конструкции
2.2 – усиленные двери и дверные коробки
2.3 – металлические решетки и жалюзи
2.4 – спецзамки, усиленные запоры
2.5 – сейфы повышенной стойкости
3 – техническая защита
3.1 – средства обнаружения радиоактивных средств
3.2 – средства обнаружения оружия
3.3 – система пожарной сигнализации
3.4 – система тревожного оповещения
3.5 – система контроля доступа
3.6- охранное освещение
3.7 – переговорные устройства
3.8 – система охранной сигнализации
3.9 – источник резервного электропитания
3.10 – система телевизионного наблюдения
3.11 – средства связи
3.12 – средства проверки почтовой корреспонденции
3.13 – средства обнаружения взрывчатых веществ
3.14 – система защиты средств ВТ и ЛВС
3.15 – средства обнаружения и защиты от технических средств проникновения через инженерные коммуникации, отверстия, проёмы и т.д.
4 – специальная защита
4.1 – обеспечение требований безопасности на этапе строительства
4.2 – проведение обследования помещений на наличие устройств съема информации
4.3 – спецпроверка технических средств передачи, обработки, накопления и хранения информации
4.4 – специальные защищенные помещения для переговоров
4.5 – средства спецзащиты сетей коммуникации

Физическая защита обеспечивается службой охраны, основной задачей которой является предупреждение несанкционированного физического проникновения на территорию, в здания и помещения объекта злоумышленников и их сдерживание в течение расчетного времени (до прибытия милиции или сил поддержки).

Инженерная защита предусматривает использование усиленных дверей и дверных коробок, металлических решеток, усиленных ограждающих конструкций, усиленных запоров, сейфов повышенной стойкости.

Техническая защита включает систему охранной сигнализации, систему телевизионного наблюдения, систему тревожного оповещения, автоматизированную систему контроля доступа, переговорные устройства, средства связи, пожарной сигнализации, средства проверки почтовой корреспонден-

ции, охранного освещения, резервного (аварийного) электропитания, систему дежурного и тревожного освещения.

Не лишним может оказаться и установка детекторов оружия (металлоискателей) и средств контроля радиационной обстановки на входе здания для предотвращения возможности проведения терактов.

Специальная защита обеспечивает защиту от утечки информации, представляющей особую ценность, **а** также проверку надежности (лояльности) персонала службы охраны, материально ответственных лиц и некоторых других категорий служащих.

Специальная защита состоит из комплекса организационно-технических и специальных мероприятий, предусматривающих:

– обеспечение требований безопасности на этапах проектирования, строительства (реконструкции) и эксплуатации зданий;

– периодическое проведение специальных обследований отдельных помещений для выявления возможно установленных в них подслушивающих устройств;

– сооружение специальных технически защищенных помещений для ведения конфиденциальных переговоров и контроль работоспособности специальных средств защиты;

– проверку и защиту технических средств, используемых для передачи, обработки, накопления и хранения конфиденциальной информации;

– оборудование средствами защиты электросети, внутренней и городской телефонной связи и других коммуникаций систем жизнеобеспечения;

– осуществление специальных проверочных мероприятий по выявлению неблагонадежных сотрудников и лиц с психическими отклонениями (автоматизированные системы психологического тестирования).

Как показывает опыт зарубежных фирм и отечественных организаций и предприятий, нормальное, безущербное функционирование возможно лишь при системном, взаимоувязанном использовании всех вышеназванных видов защиты и четко спланированных действиях сил службы охраны по сигнальной информации, получаемой от средств системы технической защиты.

1.3. Общий подход к категорированию объектов охраны

Основополагающими, определяющими выбор уровня защиты объекта, признаками являются категория важности объекта и модель нарушителя, от проникновения которого данный объект должен быть защищен.

Система охраны объекта, т.е. его периметра, территории, зданий, помещений – это сложный, многорубежный комплекс, включающий в себя физическую защиту (личный состав охраны), инженерные сооружения (решетки, стальные двери, сложные замки, замки – защелки, сейфы и т.п.), технические средства охранной сигнализации, системы телевизионного наблюдения (СТН), системы контроля доступа (турникеты, шлагбаумы, управляемые ворота и т.д.) и многое другое, что было рассмотрено в структурной схеме системы обеспечения безопасности объекта (см. рис. 1.3).

Создание технически высокооснащенной системы охраны – чрезвычайно дорогостоящее дело, поэтому разработчики КТСО и СБ (О) (исполнители и заказчики) выбирают такую конфигурацию и архитектуру КТСО, которая была бы экономически разумной. Это означает, что затраты на создание, внедрение и эксплуатацию КТСО должны быть существенно ниже, чем стоимость того, что охраняется. По некоторым оценкам эти затраты составляют около 5% основных фондов и до 25% оборотных средств в расчете на один финансовый год.

Существуют определенные методики технико-экономических обоснований выбора того или иного варианта оборудования объекта ТСОС. Однако очевидно, что для объектов особого риска, как например, ядерноопасных объектов, на которых проведение диверсионно-террористических актов может повлечь за собой неисчислимые бедствия, гибель людей, разрушение экологической системы целых регионов, требуются достаточные для их надежной защиты затраты.

Таким образом, абстрактно-типизированный подход к категорированию важности объектов (далее для краткости – категорированию объектов) необходим лишь для приближенной оценки возможных затрат на их оснащение инженерно-техническими, специальными и аппаратно-программными средствами защиты.

Второй аспект, влияющий на уровень затрат, т.е. в конце концов на выбор уровней защиты – это модель нарушителя. Например, очевидно, чем выше должностной статус злоумышленника, работающего на охраняемом объекте (например, им может быть "директор", "главный инженер" и т.д.), тем выше будут затраты на создание системы безопасности, адекватной их "моделям". Поэтому следует понимать, что абсолютной защищенности объекта быть не может. Но это уже проблемы, выходящие далеко за рамки категорирования объектов, создания и применения КТСО, хотя и в определенной мере связанные с ними.

Итак, в данном изложении определение необходимых уровней защиты мы будем связывать с понятием классификации объектов по категориям важности, полагая априори, что злоумышленник является человеком "со стороны".

В первом приближении при выборе уровня защиты следует учитывать возможность обоснованного отнесения объекта к одной из четырех категорий:

1-я категория – особо важный объект;
2-я категория – особо режимный объект;
3-я категория – режимный объект;
4-я категория – нережимный объект.

Отнесение конкретных объектов к той или иной категории важности регламентируется специальным перечнем, утвержденным правительством РФ.

В относительно самостоятельных (национальных, областных, краевых) территориальных образованиях могут создаваться свои перечни объектов,

дополняющие общий, исходя из требований местных условий и возможностей самостоятельного финансирования расходов по их оснащению КТСО.

Очевидно, что выбор уровня оснащения КТСО названных категорий объектов будет зависеть от многих конкретных факторов, как-то: конфигурация территории, рельеф местности, географическое положение, структура расположения жизненно важных центров объекта, характер угроз и т.д.

Априори следует полагать:

1-я и 2-я категории объектов требуют высокого уровня оснащения КТСО, включения в него разнообразных ТСОС, телевизионных средств наблюдения (ТСН), наличия развитой ССОИ, СКД, создания многих рубежей защиты (зон безопасности), реализации функций автоматического определения направления движения нарушителя, состояния СО, анализа характера разрушающего действия нарушителя на КТСО и т.д.;

3-я категория объектов требует меньшего, но достаточно высокого уровня оснащения. Здесь выборочно исключается исполнение ряда функций охраны (защиты), затраты на реализацию которых заведомо выше возможных потерь от злоумышленных действий;

4-я категория объектов оснащается КТСО ограниченной структуры, предполагает наличие меньшего числа зон безопасности, реализацию меньшего количества функций в ССОИ.

Следует отметить, что наряду с категорированием объектов должно применяться и категорирование помещений с организацией соответствующих "зон безопасности". Это позволит минимизировать затраты на оснащение КТСО и организацию системы защиты в целом. Выбор категории (уровня защиты) должен осуществляться исходя из значимости объекта, характера потенциальных угроз и, соответственно, "моделей" вероятных нарушителей и моделей их вероятных действий.

Приведенная классификация категорий важности объектов представляет по существу лишь укрупнено-базисный подход. В специальных разработках по этой проблеме выделяются множества подклассов, на основе чего разрабатываются идеи типизации объектов и решения соответствующих задач типизации их оснащения КТСО.

Наиболее опасной угрозой для любого объекта является угроза проведения диверсионно-террористического акта (ДТА) с применением диверсионно-террористических средств (ДТС).

Коль скоро невозможно ставить задачу защиты всех без исключения или абсолютного большинства объектов, ибо это непосильно из-за невероятно больших затрат финансовых, материальных и людских ресурсов, принят подход, в рамках которого решаются задачи определения перечня типовых особо важных объектов народного хозяйства, МО и иных (требующих охраны) объектов. Этому подходу характерна разработка рациональных (типовых) схем защиты объектов, входящих в группу риска, исходя из вероятности использования на них ДТС или их привлекательности для преступных посягательств.

Исходя из международного опыта, следует, что противодействие преступности, особенно ОПФ, может осуществляться лишь на основе государственной программы борьбы с преступностью. При этом приоритетный выбор объектов для организации системной защиты определяется, исходя из оценки возможного использования на них ДТС.

Типовые особо важные объекты, как правило, принадлежат таким отраслям как энергетика, транспорт, химические и нефтехимические, наука и техника, оборонная промышленность, оборона, связь и информатизация, а также Министерствам финансов, здравоохранения, культуры и силовым структурам страны. Эти отрасли являются ключевыми для жизнеобеспечения общества, и от их действенной защиты зависит жизнь, спокойствие и морально-психологическое состояние всего народа, прогрессивность движения общества, результативность экономических преобразований.

1.4. Классификация средств защиты

Охранная сигнализация, предназначенная для обнаружения появления различного вида угроз в любой части коммерческого объекта. В настоящее время для средних и крупных объектов создаются единые комплексные системы охранной и пожарной сигнализации.

Охранное телевидение, широко применяющееся для определения вида угрозы и ее степени, для визуального наблюдения за наиболее важными участками объекта и большими материальными ценностями.

Охранное освещение территории объекта и наиболее важных его участков внутри зданий в ночное время.

Инженерно техническая защита – усиление дверей, защита окон решетками, установка ставней и замков повышенной надежности, возведение дополнительных стен, заборов, препятствий-барьеров и т. д.

Проверка поступающей на объект корреспонденции на наличие взрывчатых веществ становится в последнее время одним из важных направлений защиты. Также проверяются въезжающие на объект автомашины персонала и посетителей.

Специальные технические средства защиты предназначены для обеспечения безопасности объекта от различных видов несанкционированного съема информации и используются:

– для поиска техники подслушивания, устанавливаемой в помещениях, в технических средствах и автомобилях;

– для защиты помещений для переговоров и других важных деловых совещаний;

– для защиты техники обработки коммерческой информации, такой как пишущие машинки, копировальные аппараты, компьютеры и др.;

– для защиты различных коммуникаций, по которым передается или циркулирует коммерческая информация.

Дополнительные средства безопасности:

– внутренняя (селекторная) телефонная связь;

– прямая (без набора) связь с ближайшим отделением милиции;

– радиосвязь с помощью переносных малогабаритных приемопередатчиков, которые используются как сотрудниками службы охраны объекта, так и персоналом, например, в крупных складских помещениях и на территории объекта;

– тревожное оповещение, которое состоит из сети звонков громкого боя, сирен и громкоговорителей, устанавливаемых на всех участках объекта для срочного оповещения условными сигналами или фразами о каких-либо видах угроз безопасности объекта. Иногда тревожное оповещение дополняется сигнальной радиосвязью, малогабаритные приемники которой имеет весь персонал. Радиосообщения от центрального поста охраны объекта поступают на эти радиоприемники, через которые передаются владельцу тональные сигналы или короткие буквенно-цифровые сообщения на небольшое табло радиоприемника.

1.5. Типовые подходы к классификации средств обнаружения и технических средств охраны

Основу комплекса технических средств охраны составляют: средства обнаружения (СО); технические средства наблюдения (ТСН); система сбора, обработки, отображения и документирования информации (ССОИ); средства контроля доступа (СКД); вспомогательные средства и устройства (блоки резервного электропитания, переговорные устройства и т.д.). Кроме того, в особо необходимых условиях применяются специальные средства защиты информации, поиска техники подслушивания, наблюдения и т.д., а также специальные средства обнаружения и обезвреживания диверсионно-террористических средств (средства защиты от ДТС).

Ниже будут рассмотрены первые три компонента, т.е. СО, ТСН и ССОИ. Остальные компоненты не могут быть рассмотрены, ибо представляют специальные области знаний, излагаемые в иных учебных программах. Отметим, что важнейшее значение для безопасности объекта имеет применение средств пожарной сигнализации, но в данной книге эти вопросы также не рассматриваются, они являются отдельным многогранным предметом изучения, которому посвящены многие литературные источники.

В инженерной практике, как правило, выделяются следующие типы СО.

1. По способу приведения в действие (постановка на охрану, снятие с охраны с центрального пульта) СО подразделяют на автоматические и автоматизированные.
2. По назначению автоматические СО подразделяют на:
   - ✓ СО для закрытых помещений;
   - ✓ СО для открытых площадок и периметров объектов.
3. По виду зоны, контролируемой СО, выделяются:
   - ✓ точечные;
   - ✓ линейные;
   - ✓ поверхностные;

- ✓ объемные (пространственные).

4. По принципу действия рассматриваются СО следующих типов:
   - ✓ механические (на практике выделяют электроконтактные, магнитоконтактные, ударноконтактные);
   - ✓ электромагнитные бесконтактные;
   - ✓ магнитометрические;
   - ✓ емкостные;
   - ✓ индуктивные;
   - ✓ гидроакустические;
   - ✓ акустические;
   - ✓ сейсмические;
   - ✓ оптико-электронные (активные и пассивные);
   - ✓ радиоволновые;
   - ✓ радиолучевые (микроволновые);
   - ✓ ольфактронные (строятся на принципе обнаружения запаха - одорологии);
   - ✓ комбинированные.

5. По количеству зон обнаружения, создаваемых СО, их подразделяют на однозонные и многозонные.

6. По дальности действия ультразвуковые, оптико-электронные и радиоволновые СО для закрытых помещений рассматривают:
   - ✓ малой дальности действия -до 12 м;
   - ✓ средней дальности действия - свыше 12 до 30 м;
   - ✓ большой дальности действия - свыше 30 м (кроме ультразвуковых СО).

7. По дальности действия оптико-электронные и радиоволновые СО для открытых площадок и периметров объектов подразделяют на:
   - ✓ СО малой дальности действия - до 50 м;
   - ✓ СО средней дальности действия - свыше 50 до 200 м;
   - ✓ СО большой дальности действия - свыше 200 м.

8. По конструктивному исполнению ультразвуковые, оптико-электронные и радиоволновые СО принято подразделять на:
   - ✓ однопозиционные - один или более передатчиков (излучателей) и приемник(и) совмещены в одном блоке;
   - ✓ двухпозиционные - передатчик (излучатель) и приемник выполнены в виде отдельных блоков;
   - ✓ многопозиционные - более двух блоков (один передатчик, два или более приемников; один приемник, два или более передатчиков; два или более приемников).

Каждый из названных классов СО представлен на рынке множеством различных датчиков, рассчитанных для применения в конкретных условиях.

1.6. Разработка концепции инженерно-технической защиты объекта

Вопрос безопасности – это компетенция руководства организации. В подготовке решения о построении системы защиты объекта обычно участвуют: руководство службы безопасности, финансовый руководитель *(финансовый директор или главный бухгалтер)*, ответственный за технические или хозяйственные вопросы.

Рекомендуется следующий алгоритм в принятии решений по созданию системы безопасности.

♦ Формулировка цели создания системы безопасности.

♦ Определение проблем, которые имеются в этой области.

♦ Формулировка требований к службе безопасности или системе безопасности.

♦ Оценка своих финансовых возможностей, рассмотрение возможной альтернативы.

♦ Обращение к услугам специализированной фирмы.

♦ Составление своих целей и возможностей с предлагаемым решением.

При выборе алгоритма необходимо:

- полагаться на профессионалов, пользоваться рекомендациями консультантов;
- обратить внимание на репутацию подрядчика;
- проявить реализм, выбирая эффективное решение, продумать, нужны ли избыточные возможности аппаратуры;
- требовать доказательств правильности принятого решения;
- учитывать, что срок службы технических средств охраны составляет в среднем 5 – 7 лет;
- принимать комплексное решение: одно уязвимое место в системе защиты может сделать бесполезными все затраты;
- учитывать, что наличие средств охраны позволяет получать скидку при страховании;
- помнить, что система защиты должна быть индивидуальна;
- учитывать, что применение современных средств охраны позволяет сократить число охранников на объекте (оптимальное число охранников на посту – 2 человека).

Инженерно-техническая защита объекта начинается с разработки концепции защиты. Концепция защиты включает в себя:

- выработку общей точки зрения по вопросам защиты объекта между руководством предприятия, службой безопасности и фирмой, предлагающей услуги в области охранной сигнализации;
- разработку принципов организации системы корпоративной безопасности на предприятии;

- определение оптимальных объемов финансирования программ инженерно-технической безопасности в соответствии с потребностью в обеспечении необходимого и достаточного уровня безопасности.

Разработка концепции инженерно-технической защиты начинается с:

- оценки вероятности актуализации отдельных видов потенциальных угроз, и попытки построения их иерархического перечня;
- решения вопроса, кем будет осуществляться физическая охрана объекта (собственными силами, силами правоохранительных органов или охранным агентством);
- определения допустимых режимных ограничений, которые не нанесут ущерба технологии основной деятельности предприятия;
- определения диапазона возможного финансирования программ, связанных с инженерно-техническим обеспечением безопасности;
- расставления приоритетов и определения ориентировочных сроков реализации программ.

Независимо от того, кто будет разработчиком концепции, ему понадобятся следующие исходные данные, которые должны будут собраны и предоставлены службой безопасности:

- подробные планы территории и поэтажные планы помещений объекта с указанием их функционального назначения и конструктивных особенностей;
- схемы внутриобъектовых коммуникаций (энергоснабжение, теплоснабжение, водопровод, телефонная связь, локальные компьютерные сети и др.) с указанием способа их прокладки;
- подробное описание уязвимых мест, для несанкционированного проникновения на объект (туннели-коллекторы тепловых и водопроводных коммуникаций, вентиляционные шахты, тонкие стены, граничащие с чужой территорией, сопредельные здания и помещения, удобные переходы с крыши на крышу и пр.);
- места, уязвимые с точки зрения жизнедеятельности объекта (электрощитовая, бойлерная, вычислительно-информационный центр (серверная), локальный телефонный узел (АТС), холодильные установки и пр.);
- условия освещения в дневное и ночное время (в том числе и аварийное освещение);
- особенности эксплуатации здания, влияющие на режим безопасности (права арендодателей помещения, необходимость посещения различными инспекциями и пр.);
- организация движения автотранспорта по территории объекта;
- ограничения по посещению отдельных зон и помещений;
- режим работы сотрудников и правила посещения клиентами.

Концепция оформляется в виде пакета документов, подписанных разработчиком, службой безопасности (при необходимости и другими службами предприятия) и утверждается первым лицом фирмы, компании, организации.

Итоговый документ концепции инженерно-технической защиты объекта должен содержать следующие материалы.

1. Анализ возможных видов угроз, расставленных в иерархический ряд на основе оценки реальной степени риска.

2. Планы зданий и территорий с графиками и маршрутами движения сотрудников и посетителей.

3. Схему расположения основных коммуникаций, и методы их защиты.

4. Схему (план) физической охраны объекта (с указанием зон режимности, расположением постов охраны и маршрутами их движения, распределение функций между постами охраны).

5. Принципиальную схему инженерно-технического оснащения объекта (системы сигнализации и контроля доступа, теленаблюдение, инженерные преграды, ловушки).

6. Рекомендации по организации контрольно-пропускного и внутриобъектового режима.

7. Инструкции по порядку взаимодействия охранных структур с правоохранительными органами,

8. Инструкции по локализации происшествий и чрезвычайных ситуаций.

9. Рекомендации по созданию системы предотвращения утечки информации с объекта.

10. Предварительную смету расходов на выполнение необходимых проектных и монтажных работ с указанием ориентировочной стоимости оборудования (или допустимые пределы расхода средств на эти цели).

11.Рекомендации по привлечению сторонних организаций для проведения необходимых работ.

В зависимости от структуры предприятия и характера выполняемых работ концепция может быть дополнена другими разделами.

1.7. Разработка концепции охраны объекта

Охрана любого объекта обеспечивается рациональным сочетанием системы технических средств и физической охраны. Физическая охрана обычно организована по постам следующим образом:

- стационарные посты (стационарный пост выполняет охранные функции, предусматривающие несение службы на строго определенном месте, как-то: КПП при входе на объект, охрана входа в объект, досмотр транспортных средств на КПП и т.д.);
- подвижной (патрульный) пост (выполняет функции по охране территории, группы помещений, периметров зданий, участков местности и т.д., осуществляет патрулирование по заданному маршруту и, как правило, по жесткому временному графику). Часто, наряду с охранными, подвижной пост выполняет инспекционные функции, например, контроль противопожарной безопасности, проверку стационарных постов);

- пост наблюдения — разновидность стационарного поста, но с задачами держать в поле зрения с помощью технических средств большое количество объектов охраны;
- "тревожная группа" или группа быстрого реагирования организуется на предприятиях с большим числом охраняемых объектов, с задачей оказания оперативной помощи стационарным или подвижным постам в случае возникновения чрезвычайных обстоятельств.
- сопровождающий пост, выполняет функции по охране людей или грузов на маршрутах следования.

Для увеличения эффективности деятельности сотрудников службы охраны используются следующие виды инженерно-технических средств:

- средства противодействия несанкционированного проникновения на объект, защитные ограждения, такие как:
  - заборы;
  - турникеты;
  - оконные решетки:
  - бронедвери;
  - замки;
  - специальные запоры;
  - сейфы;
  - бункера:
  - хранилища;
  - бронестекла;
  - защитные кабины и пр.);
- средства охранно-пожарной сигнализации, регистрирующие несанкционированное проникновение в охраняемую зону или возгорание (задымление) в ней;
- средства контроля доступа, выполняющие функции идентификации личности, проходящей через специальные контрольные пункты (регистрирующие, разрешающие или запрещающие проход человека в данное место);
- средства тревожной сигнализации (для подачи охранником сигнала тревоги при нападении на пост, или в других чрезвычайных ситуациях);
- устройства, регистрирующие пронос в охраняемую зону запрещенных материалов и изделий (источников радиоактивного излучения, оружия, взрывчатых веществ, работающей радиоаппаратуры и пр.);
- приборы акустического, оптического или телевизионного мониторинга охраняемых помещений или территории;
- контрольные устройства, регистрирующие факты несоблюдения охранниками или должностными лицами своих штатных обязанностей (например, сон на посту, отклонение от маршрута и пр.);

Необходимость наличия в составе службы безопасности службы охраны, диктуется следующими обстоятельствами:

1. Необходимость выполнения охраной функций защиты охраняемых объектов, которые нельзя возложить на технические средства.

2. Необходимость осуществления контроля за работой технических средств и поддержания их в исправном состоянии.

3. Необходимость демонстрации наличия охраны в местах, уязвимых для несанкционированного проникновения на объекты.

Таким образом, минимально необходимое количество охранников будет складываться из числа:

- постов по количеству контрольно-пропускных пунктов;
- постов слежения с использованием технических средств охранной сигнализации и наблюдения.

На современные системы инженерно-технической защиты, могут быть возложены следующие функции:

- блокировка помещений и рубежей, которые должны контролироваться с центрального поста охраны;
- профилактика попыток проникновения в охраняемые помещения лиц, не имеющих права беспрепятственного прохода или доступа в них;
- идентификация личности сотрудников и посетителей, которым предоставлено право прохода в охраняемые помещения;
- регистрация попыток проноса на территорию объекта запрещенных веществ и предметов (радиоактивные изотопы, оружие, взрывчатые вещества и пр.);
- контроль за целостностью коммуникаций и работоспособностью аппаратуры системы технической защиты;
- сбор, обработка и отображение информации, поступающей с охраняемой территории на центральный пункт охраны;
- регистрация попыток нештатного обращения с техническими средствами охраны персонала объекта и посетителей;
- выявление каналов утечки информации с объекта путем использования технических средств;
- контроль за правильностью несения службы персоналом охраны и регистрация фактов отклонения от предписанного порядка поведения во время охраны;
- накопление оперативной информации по всем событиям, связанным с обеспечением безопасности с иерархией доступа к накопленным сведениям.

Необходимость выполнения вышеперечисленных функций определяет состав требований к техническим средствам охраны и контроля.

1.8. Специальная защита высшего руководства предприятия

Внимательное изучение рынка средств специальной защитной техники и новейших разработок в этом направлении позволяет сделать вывод о практической возможности сравнительно быстрого развертывания на объекте ком-

плекса программно-аппаратных средств для дополнительного эффективного усиления защиты высшего руководства любого предприятия.

При этом могут быть реализованы следующие возможности:

1. Контроль за пользованием средствами связи и оргтехники, находящимися в кабинете руководителя во время его отсутствия.

2. Надежная регистрация (возможно в виде, скрытом от окружающих) фактов посещения кабинета в неурочное время с возможностью фиксации действий посетителя на видео- или фотопленку.

3. Автоматическая или принудительная запись любого разговора хозяина кабинета с посетителем лично или по телефону для использования в дальнейшем для расследования фактов угроз или для целей анализа.

4. Устройство скрытого в интерьере кабинета хранилища документов сейфового типа.

5. Усиление защищенности имеющихся сейфов и дверей как от грубых методов взлома, так и изощренного вскрытия (защитные замковые накладки, ловушки для отмычек, спецметки, защита от методов интроскопии).

6. Оперативная регистрация проноса в кабинет радиоактивных изотопов с возможностью оценки интенсивности гамма и бета-излучений.

7. Регистрация наличия оружия и средств скрытой звукозаписи при помощи специально оборудованных кресел для посетителей.

8. Устройства для регистрации попыток обыска ящиков стола, книжных шкафов и других предметов интерьера, осуществляемых лицом, проникшим в кабинет.

9. Возможность подачи сигнала тревоги при попытках:

- вскрыть сейф или другое хранилище;
- добраться в базу данных персонального компьютера:
- заноса радиоактивных веществ или оружия;
- выноса специально обработанного предмета на расстояние свыше одного метра от своего постоянного места.

10. Обеспечение защиты от перехвата разговоров и факсимильных сообщений по телефонным линиям.

11. Защитные меры по нейтрализации возможных каналов утечки информации из кабинета:

- выявление радиопередающих и звукозаписывающих закладок;
- акустическое зашумление кабинета;
- создание электромагнитной завесы.

12. Обеспечение скрытого контроля за конкретным помещением (например, комната переговоров).

Все указанные средства могут быть объединены в единую локальную сеть персонального компьютера в кабинете с возможностью гибкого программирования режимов работы каждого аппарата и накопления информации для анализа и расследования.

1.9. Должностные обязанности субъектов управления корпоративной безопасностью по действиям в кризисных и чрезвычайных ситуациях

Чтобы минимизировать потери от всяких происшествий, стихийных бедствий и любых чрезвычайных ситуаций, очень полезно иметь специально разработанные планы или другие документы, которые внесли бы хоть какое-то организующее начало в возникающей неразберихе и панике.

Очень полезны, например, инструкции, заложенные в электронную память ряда современных систем охранной сигнализации и автоматически выводимые на экран монитора при поступлении сигналов тревоги, сигналов о неисправности или других сообщений. Некоторые виды таких инструкций являются обязательными (планы эвакуации при пожаре), некоторые могут задаваться, к примеру, правоохранительными органами при заключении договора на охрану. Но в любом случае, чем больше возможных ситуаций будет охвачено, тем меньше потерь будет при их локализации.

Желательно проработать такие ситуации, как:

- нападение на объект:
- захват заложников;
- угрозы персоналу охраны;
- стихийные бедствия (наводнение, ураган, землетрясение);
- аварии систем жизнеобеспечения;
- несчастные случаи на объекте.

Необходимо учитывать при разработке планов обязательные требования нормативных документов, в частности, Постановления Правительства Российской Федерации от 3 июня 1995 года № 558 "Об утверждении положения о порядке расследования и учета несчастных случаев на производстве'", которое устанавливает единый порядок поведения должностных лиц в подобной ситуации, а следовательно, налагает определенные обязанности на дежурную службу. Такой кризисный план прежде всего будет способствовать пониманию необходимости решения общей задачи локализации происшествия, без чего трудно решать уже частные задачи.

При разработке вышеуказанных планов должны быть составлены схемы связи, вызова и оповещения сотрудников в подобных ситуациях (особенно, кому это предписано должностными обязанностями).

2. СИСТЕМЫ И СРЕДСТВА ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ

Инженерно-техническая защита включает в себя средства отражения, противодействия появлению и развитию различного вида угроз. В ее состав входят естественные и искусственные препятствия на территории объекта, такие элементы систем разграничения доступа, как металлические двери, шлюзовые камеры, сейфовые помещения, соответствующим образом оборудованные посты охраны, металлические решетки, защитные пленки на окнах и т.п.

Естественные препятствия желательно использовать при архитектурном проектировании объекта: водные преграды, овраги, пустоши, колючие и трудно проходимые заросли и т.п.

Искусственные препятствия:

1) периметрические ограды (заборы):

– прозрачные – из колючей проволоки, металлических сеточных или решетчатых секций;

– непрозрачные – деревянные, кирпичные или бетонные;

2) ограничители направления и скорости проезда автотранспорта – ворота, шлагбаумы, "лежачие полицейские", "стиральная доска", быстро выдвигающиеся из полотна дороги бетонные или стальные эскарпы.

Высота ограды обычно не превышает 2-2,5 м. В особо ответственных случаях может быть установлено две и более линий ограждения на расстоянии 1,5-2 м друг от друга, пространство между которыми контролируется системами охранной сигнализации и теленаблюдения.

Сложные системы естественных и искусственных препятствий оказывают значительное психологическое давление на нарушителя и способны отпугнуть малоподготовленного злоумышленника, а подготовленного вынудить совершать ошибки и терять время.

Противодействие угрозам стихийных бедствий (пожар, затопление, землетрясение) осуществляется путем использования специальных каркасных конструкций, усиления стен, полов и потолков наиболее важных помещений, герметизации хранилищ материальных и информационных ценностей.

2.1. Зоны безопасности

Важнейшим средством инженерно-технической защиты является планировка объекта, его зданий и помещений по зонам безопасности, которые учитывают степень важности различных частей объекта с точки зрения их возможного ущерба.

Основа концепции защиты объекта – оптимальное расположение зон безопасности и размещение в них постов физической охраны и эффективных технических средств обнаружения, отражения и ликвидации угроз.

Расположение зон безопасности на объекте приведено рис. 1.4.

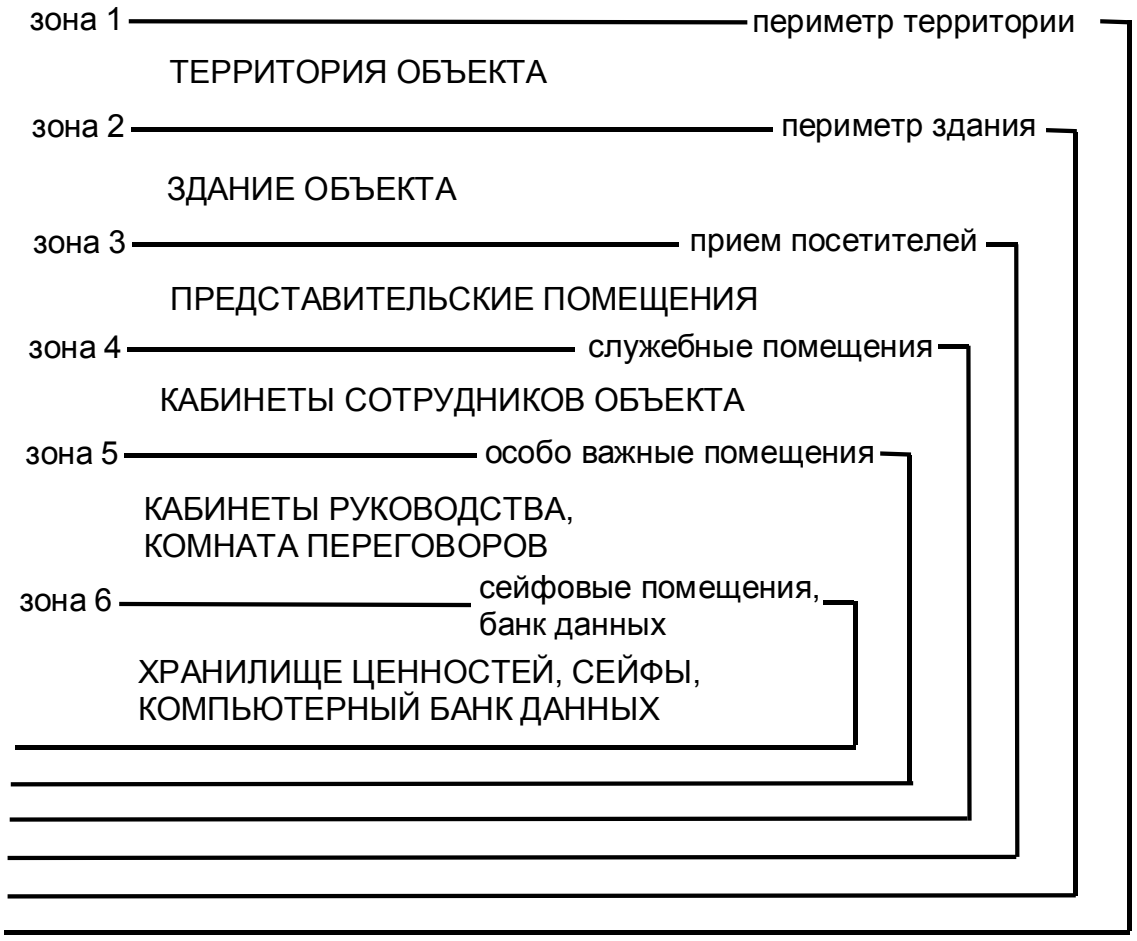

Рис. 1.4 – Схема расположения зон безопасности

Зоны безопасности следует располагать на объекте последовательно ("концентрически"): от периметра территории до хранилища ценностей и информации, создавая каскадирование препятствий, которые придется преодолевать нарушителю.

Отметим, что граница зоны безопасности одного уровня должна быть равнопрочной, т.е. у нее должны отсутствовать явно слабые и тем более незащищенные места, иначе зона будет легко и быстро преодолена злоумышленниками через слабо защищенный участок.

2.2. Системы управления доступом

Системы охранной сигнализации функционируют, как правило, в нерабочее время, для повышения безопасности в рабочее время необходима эффективная система контроля за помещениями, сотрудниками и посетителями. При этом сотрудники, обладающие необходимыми полномочиями, должны чувствовать себя свободно и иметь возможность перемещаться по зданию или территории объекта без помех. Эта задача и решается с помощью систем управления доступом (СУД).

Понятие "контроль и управление доступом" можно определить как комплекс мероприятий, направленных на ограничение и санкционирование перемещения людей, предметов, транспорта в помещениях, зданиях, сооружениях и по территории объектов.

С системами управления доступом мы сталкиваемся по несколько раз в день. Уходя утром на работу, закрывая дверь, ограничиваете доступ посторонних в Ваш дом. Вошли в метро, показали проездной – прошли через турникет. Вечером пришли домой, вставили ключ в замок – вошли, Ваш ключ дает Вам право войти в свою квартиру.

Естественно, системы, управляющие доступом, очень разнообразны и не похожи друг на друга. Есть обычные навесные амбарные замки, а есть электронные средства охраны, которым не нужны деньги и женщины, которым не страшен мороз и работа по 24 часа в сутки, которые не имеют пристрастий и вредных привычек. Исследования показывают, что во время массового прохода, в часы пик, человек-контролер контрольно-пропускного пункта пропускает до 25% лиц с дефектными и чужими пропусками. После четырех часов работы величина ошибки возрастает до 40%. И не случайно, что именно электронные системы управления доступом работают в крупных аэропортах, банках, гостиницах, ядерных научных центрах, военных базах, т.е. везде, где серьезно подходят к безопасности.

Это совсем не значит, что человеку нет места в современной системе охраны. Есть, но строго определенное: реагирование на сигнал тревоги, общее наблюдение и управление в нестандартной ситуации.

Конечно же, большинство СУД не может обойтись без персонального компьютера (ПК). Для системы, обслуживающей больше десятка дверей, ПК просто необходим. Иначе можно утонуть в море информации и не обеспечить надлежащего уровня охраны.

Вообще, применение ПК – это качественно новый этап развития СУД. Используя компьютер, служба безопасности сможет создавать и пополнять базу данных пользователей, в которую заносятся фото и биографические данные сотрудников, вести учет происходящих событий, составлять всевозможные сводки, координировать работу всех систем безопасности объекта, а самое главное – в максимально удобной форме отображать ситуацию, происходящую на объекте.

Есть, к примеру, программные средства, которые автоматически выбрасывают на экран монитора фотографию проходящего через турникет или шлюз человека, на имя которого зарегистрирована карта. Охранник посмотрит на монитор, посмотрит на пользователя, который в этот момент проходит мимо бронированной кабинки, где сидит охранник, и если лица совпадают, подтвердит разрешение на проход.

Или еще одна очень распространенная программа – тревожная графика. На поэтажные планы охраняемого объекта наносят стандартные элементы системы охраны: подконтрольные двери, датчики сигнализации, телевизионные камеры. Выбирая иконки, оператор может открывать/закрывать двери, выводить на монитор ту или иную телекамеру и т.д. В случае поступления

сигнала тревоги автоматически на монитор выводится план этажа и выделяется место, откуда тревога поступила.

Кроме поддержания охранных функций, программное обеспечение очень удобно использовать для ведения административного учета. По желанию администрации система может автоматически отслеживать все перемещения сотрудников по объекту. Это позволяет построить систему учета рабочего времени и в случае необходимости быстро определить местонахождение нужного сотрудника.

Хорошее программное обеспечение позволяет организовать в сетевой среде несколько рабочих станций с распределенными функциями управления (компьютеры службы безопасности, администратора предприятия, отдела кадров).

Сегодня СУД широко применяются как дополнение к существующим системам защиты и охраны. Многие зарубежные фирмы представляют на российский рынок различные модели СУД. Кроме того, ряд отечественных организаций работают над созданием систем управления доступом с применением определенных компонентов и устройств ведущих европейских, американских, японских и других фирм.

Вместе с тем, выбор технических средств носит в определенной степени случайный характер, так как потребитель часто имеет представление о СУД только по рекламным проспектам, что в конечном итоге приводит или к неоправданным денежным затратам или к неэффективному использованию систем. Для обоснования применения новых технических средств охраны необходимо иметь справочную и методическую литературу, а также нормативные документы, рассматривающие вопросы выбора, применения СУД и представляющие базу для сертификации как отдельных устройств, так и систем в целом.

СУД – самое интенсивно развивающееся направление в технике обеспечения безопасности. Это связано с целым рядом факторов.

Во-первых, СУД могут обеспечить полную автоматизацию контроля и управления доступом, что в общем случае приводит к экономии средств на обеспечение безопасности.

Во-вторых, СУД могут решать такие задачи, как учет рабочего времени, быстрое определение местонахождения сотрудника, управление лифтами, освещением, вентиляцией и т.д.

В-третьих, системы охранной сигнализации функционируют, как правило, в нерабочее время, при этом двери, окна и заграждения закрыты. В рабочее же время система охранной сигнализации отключена, большинство входов открыто, что позволяет свободно перемещаться служащим, посетителям, а также возможным нарушителям. Следовательно, для повышения безопасности в рабочее время необходима эффективная система контроля за помещениями, сотрудниками и посетителями. При этом сотрудники, обладающие необходимыми полномочиями, должны чувствовать себя свободно и иметь возможность перемещаться по зданию или территории объекта без помех. Эта задача и решается с помощью СУД.

Технические средства СУД включают в себя механические, электромеханические, электрические, электронные конструкции, устройства и программные средства, обеспечивающие реализацию контроля и управления доступом.

В основе работы СУД заложен принцип сравнения тех или иных идентификационных признаков, принадлежащих конкретному физическому лицу или объекту, с заложенными в памяти системы. Каждый из пользователей (сотрудников) получает индивидуальный идентификатор с кодом (карту, брелок или другой подобный предмет).

Идентификатор может быть закреплен на определенном предмете и транспортном средстве. В качестве идентификационных признаков могут использоваться также биометрические данные человека (отпечатки пальцев, геометрия кисти руки, голос и т.д.). У входа в контролируемое помещение устанавливаются специальные устройства, считывающие информацию с идентификатора или биометрические показатели. Далее информация поступает в систему, которая на основании анализа данных о владельце реагирует соответствующим образом: открывает или блокирует дверь, включает сигнал тревоги, регистрирует присутствие человека на рабочем месте и т.д.

Кроме того, СУД могут обеспечить множество дополнительных возможностей, например:

- сбор и обработку информации о перемещении лиц и предметов по объекту;
- организацию и учет рабочего времени; управление освещением, лифтами, вентиляцией и другой сервисной автоматикой:
- управление автоматикой автостоянок; поддержку различных функций охранной и пожарной сигнализации;
- управление приборами телевизионной системы наблюдения.

Основные функции СУД:

- санкционирование – процедура присвоения каждому пользователю персонального идентификатора, регистрацию его в системе (или регистрацию его биометрических признаков) и задание для него временных интервалов и уровня доступа (в какие помещения и когда он имеет право заходить);
- идентификация – процедура опознавания пользователя по предъявленному идентификатору или биометрическому признаку;
- аутентификация – установление подлинности пользователя по предъявленному идентификатору;
- авторизация – проверка полномочий, заключающаяся в проверке соответствия времени и уровня доступа установленным в процессе санкционирования;
- разрешение доступа или отказ в доступе – выполняется на основании результатов анализа предыдущих процедур;
- регистрация – протоколирование всех действий в системе;
- реагирование – реакция системы на несанкционированные действия (подача предупреждающих и тревожных сигналов, отказ в доступе и т.д.).

Процедура санкционирования производится оператором или администратором системы и заключается во вводе необходимых данных в компьютер системы или в контроллер. Все остальные процедуры могут делаться системой автоматически. Очевидно, что процедура аутентификации может быть выполнена полноценно только с помощью биометрической идентификации, так как идентификатор-предмет можно передать другому лицу.

Очень интересна интеграция СУД с системами охранно-пожарной сигнализации (ОПС) и телевизионных систем наблюдения (ТСН). Можно выделить два наиболее общих уровня – интеграцию с системами ОПС и ТСН на релейном уровне и интеграцию на системном уровне.

Релейный уровень предполагает наличие дополнительного модуля в контроллере (или дополнительных входов/выходов в контроллере), к которому подключаются охранные или пожарные извещатели**,** и релейных выходов для управления телекамерами и другими устройствами.

Системный уровень предполагает подключение к общей магистрали (каналу связи, сети) отдельных контроллеров (охранных панелей, контроллеров управления ТСН).

Соответственно должно быть специальное программное обеспечение, поддерживающее интеграцию.

Анализируя современные сетевые СУД, можно определить, что они строятся на основе компьютерных сетей, а также на основе локальных сетей различного уровня сложности специальных вычислительных устройств – контроллеров. Возможны четыре уровня сетевого взаимодействия элементов СУД:

1) компьютерная сеть типа клиент/сервер на основе сети INTERNET, с протоколом обмена TCP/IP и с использованием сетевых операционных систем Windows NT или Unix. Этот уровень обеспечивает связь между сервером и рабочими станциями операторов.

2) связь между контроллерами и компьютерами подсистем. На этом уровне используется интерфейс RS-232.

3) связь между контроллерами и считывателями. Здесь применяется интерфейс RS485 или, ставшие уже стандартом, интерфейсы считывателей Weigand**,** магнитных карт.

4) извещатели ОПС и цепей управления – сбалансированные и несбалансированные радиальные шлейфы, релейные выходные цепи, адресные шлейфы. Здесь, как правило, применяются нестандартные специализированные интерфейсы и протоколы обмена информацией.

Замечания по поводу интеграции систем безопасности:

- полная интеграция систем нецелесообразна, эти системы должны работать автономно, а возможно и дублировать друг друга в некоторых функциях, что обеспечивает более высокую "живучесть" системы безопасности в целом;
- полностью передавать управление системой компьютеру нельзя, так как компьютер наименее надежное звено системы. Для обеспечения высокой надежности необходимо применять специализированные компьютеры, а

также использовать различные методы резервирования. Элементы системы должны иметь распределенный интеллект, чтобы обеспечить автономное выполнение своих основных функций;

- сеть верхнего уровня должна быть локальной, физически отделенной от остальных информационных сетей объекта, и для передачи данных в ней необходимо использовать криптографические методы защиты информации, а также имитостойкие протоколы обмена информацией.

Анализ совместного применения СУД и средств ОПС показывает, что в отечественной практике в большинстве случаев СУД применяется как самостоятельная система, и она часто рассматривается только как средство усиления режима обеспечения безопасности объекта. В то же время, управление доступом является фундаментальным понятием процесса обеспечения безопасности. В любой системе охранной сигнализации присутствуют элементы контроля доступа. Они используются для обеспечения взятия и снятия объекта под охрану. Переход систем охранной сигнализации на автоматический режим работы (постановка объекта под охрану и снятие объекта с охраны производится пользователем) потребует введения в систему охранной сигнализации полноценных элементов контроля доступа, а развитые СУД уже имеют в своем составе модули, позволяющие обеспечить подключение охранных и пожарных датчиков. Поэтому СУД в настоящее время можно рассматривать как основу для создания интегрированных систем обеспечения безопасности.

2.3. Классификация СУД

Предлагаемая классификация систем управления доступом достаточно условна. При ее создании учитывались только самые базовые характеристики: количество пользователей, число дверей, обслуживаемых в максимальной конфигурации, возможность взаимодействия с системами сигнализации и теленаблюдения, работа в сети и с использованием компьютера.

Цель классификации – помочь разобраться в многообразии СУД и не сделать грубых, трудноисправимых ошибок при выборе системы для конкретного объекта.

По структуре СУД можно классифицировать по нескольким основаниям.

По условиям функционирования:

- автономные – для управления одним или несколькими заграждающими устройствами без передачи информации на центральный пункт охраны и без контроля со стороны оператора;
- сетевые – для управления заграждающими устройствами с обменом информацией с центральный пунктом охраны и контролем, управлением системой со стороны дежурного оператора.

По структуре и выполняемым функциям СУД можно классифицировать следующим образом.

Однодверные системы

При необходимости контролировать только одну дверь следует сразу определиться, нужно ли будет в дальнейшем расширять систему или конфигурация будет окончательной.

Оснащение одной двери – это только первый шаг к созданию СУД объекта. В этом случае, думая о будущем развитии, используют специально созданные одно- или двухдверные контроллеры, которые при необходимости могут легко интегрироваться в более мощную систему. Чаще всего к контроллеру можно подключить до двух считывателей, которые устанавливают на две двери или на одну для контроля входа и выхода. Один из считывателей можно заменить на клавиатуру для набора кода.

В некоторых исполнениях считыватель и контроллер объединены в один корпус. То есть блок, принимающий решение об открытии замка, сосредоточен в считывающем модуле. Это, с одной стороны, удешевляет систему, но с другой – уменьшает функциональные возможности, а главное, увеличивает вероятность взлома.

В еще более дешевых системах совмещаются в одном корпусе принимающий решение блок, клавиатура для набора кода, считыватель и замок. Чаще всего в однодверных системах используются считыватели магнитных карт, Touch Memory , реже – биометрия, проксимити, Wiegand и другие.

Но в большинстве однодверных систем считыватели совмещены с клавиатурой для набора индивидуального кода. С помощью клавиатуры осуществляется программирование систем.

Что делать, если возникла необходимость увеличить число обслуживаемых дверей?

1) Ряд систем позволяют объединить контроллеры в единую сеть. Как правило, для этого используется специальный модуль связи, который вставляется в корпус контроллера. Но такое объединение не может быть продолжено до бесконечности. Хотя контроллеры и обмениваются некоторыми данными, они, по сути, остаются автономными и при программировании придется ходить от двери к двери и вводить одну и ту же информацию.

2) Повышение уровня системы – Upgrade. При желании расширить систему вызываете специалистов фирмы-инсталлятора. Они снимают старые автономные контроллеры и устанавливают новые сетевые. Скорее всего, за это придется платить, хотя сумма будет гораздо ниже, чем при установке новой системы. При этом важно, что считыватели и коммуникации не меняются, что удобно при монтаже устройств на работающем объекте.

Системы малой и средней емкости

Системы емкостью до 16 дверей строятся на основе одного или нескольких последовательно соединенных контроллеров. Число контроллеров зависит от емкости системы и максимального количества считывателей, обслуживаемых одним контроллером.

Как правило, для увеличения эффективности работы и уменьшения стоимости всей системы безопасности объекта СУД малой емкости позволяют осуществлять интеграцию с датчиками сигнализации.

Особенность систем средней емкости – существенное увеличение числа пользователей и количества обрабатываемой информации. В связи с этим, использование персонального компьютера в таких системах обязательно. Компьютер и программное обеспечение позволяют программировать каждый контроллер, собирать и анализировать информацию, составлять всевозможные отчеты и сводки, более эффективно отслеживать ситуацию на объекте.

За редким исключением такие системы легко расширяются. Каждый контроллер работает независимо от остальных и поэтому содержит базу данных на всех пользователей.

Средние системы не привязаны к конкретной технологии. Специальные адаптеры (преобразователи) кода позволяют подсоединить считыватели различных технологий. Многие производители даже заявляют о том, что их система интегрируется с любым считывателем. Но, как правило, либо это утверждение недостаточно обоснованно, либо требует серьезных дополнительных затрат на установку новых модулей.

Системы большой емкости

Отличительные особенности больших систем: наличие развитого программного обеспечения, позволяющего реализовать большое число различных функциональных возможностей, и способность СУД к осуществлению высокой степени интеграции с другими системами объекта.

Системы большой емкости строятся на основе разветвленной сети контроллеров. Число пользователей в этом случае исчисляется уже десятками и сотнями тысяч, поэтому создается общий банк данных, и контроллер, давая разрешение на проход, обменивается информацией с центральным компьютером. Причем, если произошло разрушение сети, то система, как правило, не прекращает работы, каждый контроллер функционирует в автономном режиме и пользуется только базой данных, заложенной непосредственно в него, без обмена информацией с соседями и компьютером.

Еще одна отличительная особенность системы такого класса – возможность связи входных и выходных устройств разных контроллеров системы. Например, можно запрограммировать систему так, чтобы срабатывание датчика сигнализации у входа в офис, вызывало блокирование электрозамков, подключенных к нескольким контроллерам, контролирующим близлежащие помещения.

Кроме того, программное обеспечение больших систем позволяет использовать для управления сразу несколько компьютеров и распределить между ними функции. Большие системы, как правило, работают в самом тесном взаимодействии с другими инженерными системами объекта: охранной сигнализацией, охранным и технологическим телевидением, с системами жизнеобеспечения, оперативной связи и др.

2.4. Принципы построения и элементы СУД

Обычно система управления доступом состоит из:

- набора карт-пропусков (идентификационных ключей), которые выдаются пользователям системы;
- считывателей – устройств, идентифицирующих ключи;
- исполнительных устройств, которыми могут быть электрозамки, шлагбаумы и электроприводы ворот любых типов;
- контроллеров – интеллектуальных блоков, управляющих системой и принимающих решение о возможности прохода.

Любая система управления доступом начинается с ключей (носителей идентификационных признаков), т.е. с тех элементов, которые раздаются пользователям системы и содержат в себе индивидуальный признак пользователя.

В качестве ключей-носителей признака могут использоваться карты различных типов: магнитные, вигаид, проксимити, или же сам человек, как носитель индивидуальных биологических признаков, человеческая память, запоминающая набор цифр, которым является PIN-код (индивидуальный код пользователя) и др.

Для съема информации с ключей предназначены устройства идентификации. В зависимости от типа носителя, естественно, меняются и устройства идентификации. Съем информации с различного вида карт осуществляют специальные считыватели, использующие те или иные физические принципы. Для съема информации о биологических признаках человека используют специальные биометрические считыватели (терминалы), а ввод PIN-кода осуществляется с клавиатур различных типов.

Информация, снимаемая с ключей, поступает в процессорный блок – контроллер, который ее обрабатывает, анализирует и принимает решение о возможности прохода. Любая система обязательно имеет плату, на которой размещается микропроцессор и другие полупроводниковые элементы. Другой вопрос, где эта плата расположена: в отдельном блоке-контроллере, или она вставлена прямо в корпус считывателя. У каждой из этих архитектур есть свои плюсы и минусы. Архитектура контроллера, совмещенного со считывателем, более устойчива к обрывам сети, но и менее защищена от взлома, т.к. блок, принимающий решения, расположен вне охраняемого помещения.

СУД может взаимодействовать с персональным компьютером. В системах достаточно большой емкости компьютер, используя специализированное программное обеспечение, полностью управляет контроллерами, собирает, обрабатывает и архивирует информацию, поступающую с объекта, осуществляет взаимодействие с сигнализацией и охранным телевидением.

2.5. Устройства идентификации

Смарт-карты

Технология изготовления смарт-карт (smart) появилась в 1976 году. В этом году компания «CP8 Transac» (концерн «Bull») объявила о выпуске первой в мире пластиковой карты со встроенной микросхемой. Смарт-карта представляет собой пластиковую карточку, по размерам соответствующую

обычной кредитной карточке, в которую заключены микропроцессор и запоминающее устройство.

Внутренняя архитектура смарт-карты включает микропроцессор, позволяющий использовать сложные способы кодирования информации, постоянную память (ROM), в которую зашиты команды для процессора, оперативную память (RAM), используемую в качестве рабочей, и перезаписываемую память (EEPROM) для чтения и записи информации извне.

Объем памяти достигает 1 MB, что позволяет обеспечить высокую криптозащищенность данных и их изменения.

Основным преимуществом смарт-карт является большой объем памяти и высокая защищенность информации от попыток модификации и дублирования.

Основной недостаток удостоверений такого типа – их высокая стоимость, поэтому в системах управления доступом, применяемых в России, они используются крайне редко. К тому же, главное достоинство смарт-карт – криптозащитный механизм изменения данных – для организации управления доступом в помещения в общем-то и не нужен.

"Таблетки" Touch Memory (фирма"Dallas Semiconductor")

Термин «Touch Memory» можно перевести (дословно – «касание памяти») как «моментальное считывание информации, записанной в памяти идентификатора». По месту разработки эти идентификаторы еще называют «даллаские таблетки», а с 1997 года -«iButton» (интеллектуальные таблетки).

Touch Memory были разработаны американской компанией «Dallas Semiconductor». Эти устройства физически представляют собой микросхему, размещенную в прочном корпусе из нержавеющей стали**,** внешне напоминающем батарейку от электронных часов диаметром 16,3 мм и высотой 5,8 (3,2) мм.

Для идентификации необходимо прислонить таблетку к считывателю, который имеет два считывающих контакта – один для передачи данных, второй – «земляной». Информационный обмен с контроллером осуществляется по двухпроводной линии. Время считывания около 0,1 с. Длина кода 8+48+8 бит.

Все идентификаторы обеспечивают обмен данными по сети MicroLAN**.** Идентификаторы с перепрограммируемой памятью (например, DS1991/92/96 и т.д.) питаются от литиевой батареи, которой хватает на 10 лет.

Среди достоинств систем Touch Memory можно выделить: компактность; высокую стойкость к механическим повреждениям (выдерживают статическую нагрузку до 11 кг), коррозии, перепадам температур (от –40 до +70 или 85 °С); достаточно высокую скорость считывания и сравнительно небольшую стоимость системы. Различные модификации Touch Memory могут содержать встроенные часы или термометр.

В настоящее время появилась новая модель – DS1954 со встроенным криптографическим ключом длиной 1054 бит, что в принципе должно повысить защищенность системы.

Но разработчик ('"Dallas Semiconductor", США) не предполагал использовать этот класс идентификаторов в '"серьезных" пространственно разнесенных системах управления доступом. Таблетки Touch Memory используются как электронные ключи для ограничения доступа к компьютеру или в автономных однодверных замках. В системах с повышенными требованиями к безопасности Touch Memory либо не применяются вовсе, либо используются в комбинации с другими средствами (в простейшем случае дополнительно ставятся клавиатуры с PIN- кодом).

Главный недостаток – наличие контакта с гальванической связью с микроконтроллером. Другими словами, система не имеет считывателя как такового, отсюда сравнительно невысокая стойкость к вандализму и негативное влияние статического электричества. Известны случаи вывода системы из рабочего состояния при помощи электрошока (надо заметить, что при достаточно высоком уровне подготовки разработчика блока считывания этот фактор может быть практически сведен к нулю).

В России Touch Memory достаточно распространены. Популярность этих идентификаторов вызвана их более низкой, по сравнению с другими идентификационными системами, стоимостью и простотой эксплуатации. На отечественном рынке представлено более десятка различных систем на основе Touch Memory: "Dallas Lock", "Аккорд", "Менуэт", "Полонез" и др.

Штриховой код

Штриховой (линейный или BAR) код был разработан еще в 1932 году, но широкое распространение получил только с развитием вычислительной техники. Штриховой код представляет собой группу параллельных линий различной ширины, наносимых на поверхность карты. На сегодняшний день штрих-код – самая дешевая технология изготовления карточек. Карточки можно печатать на обычном офисном принтере или даже рисовать от руки.

Считыватель является фоточувствительным элементом, мимо которого просто проводится карта и он считывает код.

Штриховой код редко используется в системах управления доступом**,** но он получил широкое распространение в системах контроля технологических процессов, для автоматизации почтовых услуг, для учета товаров в магазинах и на складах.

Главный недостаток – простота подделки. Штрих-код можно скопировать на ксероксе. В более сложных модификациях штриховой код заклеивают особой пленкой, непрозрачной для человеческого глаза и прозрачной для инфракрасного света. В настоящее время такой метод маскировки штрихового кода получил широкое распространение, но, к сожалению, стоимость таких карт со штрих-кодом заметно возросла.

Лидером в производстве оборудования для штрихового кодирования информации является концерн "UBI" (Швеция). Эта компания выпускает специализированные термопринтеры и считывающие устройства: ручные оптические карандаши, оптические и лазерные сканеры и т.д.

Магнитные карты

Цифровые магнитные коды широко применяются в коммерческих кредитных карточках (VISA, STB-card и т.д.). Двоичный код наносится на полоску магнитного материала, расположенную параллельно краям карточки. Эти данные считываются при перемещении карточки вдоль считывающей головки регистрационного устройства. Хотя способ записи информации на магнитные карты стандартизован, тем не менее не все карточки и считыватели совместимы.

Стандартом разрешается для записи использовать три дорожки. Первая применяется в некоторых (довольно экзотических) банковских системах, например "Dinner's Club"'; вторая – во всех широко распространенных; третья дорожка может использоваться для записи произвольной информации. Как правило, в системах управления доступом используется вторая дорожка.

Применение алфавитных и цифровых знаков при магнитном кодировании позволяет записать на удостоверении как имя и фамилию служащего, так и номер удостоверения.

Подделка таких удостоверений не представляет особых затруднений, так как данные, записанные на магнитной полоске, могут быть расшифрованы или скопированы с помощью оборудования, выпускаемого коммерческими предприятиями. Тем не менее, эта проблема может быть частично решена путем использования особых, нестандартных методов шифровки информации и считывания кодов.

Другие существенные недостатки карте магнитной полосой:

- незащищенность от электромагнитного воздействия. Всю информацию можно стереть, оставив карту близ источника электромагнитного излучения;
- незащищенность от механического воздействия. Карту можно поцарапать ключом, находящимся в одном кармане с картой;
- быстрый износ карты от частых контактов со считывающей головкой (да и сама считывающая головка в среднем выдерживает порядка 150 – 200 тысяч проходов);
- необходимость вставлять карту в считыватель определенным образом, а в спешке это может не получиться с первого раза, поэтому в народе магнитные считыватели называют "тест на трезвость".

Оптический код

Оптический код представляет собой определенную конфигурацию точек, расположенных на вкладыше, запрессованном в карточку-удостоверение или светопроницаемом материале. Фотоэлементы считывающего устройства регистрируют изменения освещенности при просвечивании оптического кода и определяют взаимное расположение точек, образующих код.

Для того чтобы оптический код было трудно скопировать, расположение точек может быть замаскировано пленкой, непрозрачной для обычного света и прозрачной для инфракрасных лучей.

В качестве примеров одной из разновидностей оптического кода можно привести хорошо известные жетоны московского метрополитена или инфракрасные карточки компании "TDSi".

Виганд-карты

Виганд-карты изготавливают запрессовыванием внутрь пластиковой карты двух рядов кусочков проволоки из особого ферромагнитного сплава. Этот сплав найден в 1975 г. американским ученым Джоном Вигандом (Weigand), в честь которого и назван. Сплав имеет практически идеально прямоугольную петлю гистерезиса с достаточно большой амплитудой.

Считыватель представляет собой индукционную катушку с двумя магнитами противоположной полярности. Когда карта перемещается вдоль считывателя, один магнит детектирует проволочки из одного ряда, второй – из другого ряда. Один ряд дает положительные всплески индукционного тока в катушке, которые трактуются как единицы, другой – отрицательные, которые трактуются как нули. В результате с карты считывается двоичный код.

Преимущество по сравнению с магнитными картами – лучшая износостойкость, неподверженность электромагнитному излучению, высокая защищенность от подделки (состав сплава хранится в секрете, права на изобретения купила американская корпорация "Echlin", ведущий производитель – фирма "Sensor Engineering").

Проксимити-карты

Проксимити-карты предназначены для дистанционного считывания кодовой информации. В переводе на русский "proximity" означает "близость". Но близость эта довольно условна, расстояние между считывателем и картой зависит от мощности считывателя и типа карты и варьируется от 5 см до нескольких метров.

Проксимити-считыватель постоянно посылает радиосигнал. Карта при попадании в зону действия считывателя принимает его излучение и в ответ посылает сигнал, содержащий записанный на карте код.

Проксимити-карты делятся на активные и пассивные. Питание передатчика активных карт осуществляется от встроенной батарейки питания. А пассивные карты посылают сигнал за счет накопления энергии электромагнитного поля считывателя. Естественно, что расстояние срабатывания активной карты больше, чем пассивной. Кроме того, активные карты можно перепрограммировать, в то время как на пассивные карты информация записывается только один раз. Это свойство часто используется для выдачи временных и гостевых пропусков. Но за плюсы приходится расплачиваться уменьшением срока службы, сужением температурного диапазона и удорожанием. Стоимость системы пропорциональна дальности считывания.

В зависимости от используемого передатчиком диапазона частот все проксимити-карты можно условно разделить на две группы. Низкочастотные передающие устройства работают в диапазоне от 33 КГц до 500 КГц, а высокочастотные – от 2,5 МГц до 10 ГГц.

Проксимити-карты могут существенно различаться и по используемой технологии записи идентификационного кода.

Варианты технологии записи и считывания:

- использование эффекта поверхностной акустической волны;
- использование интегральных схем;
- использование схем с электрической настройкой. В таких устройствах код записывается в виде запрессованных в пластиковую карточку электрических схем, имеющих резонансную частоту. Считывающее устройство постоянно сканирует весь диапазон рабочих частот и принимает сигналы, поступающие от резонирующих электросхем, встроенных в проксимити-карты.

Достоинства проксимити-систем:

- возможность контроля за перемещением не только людей, но и предметов, автотранспорта и т.д.;
- бесконтактное считывание, т. е. зачастую карту не нужно даже вынимать из сумки или кармана;
- благодаря отсутствию контакта между картой и считывателем, срок службы пассивных карт неограничен, правда, активные карты через 5 лет требуют замены батарейки (если это возможно);
- высокая защищенность от подделки;
- проксимити-системы обеспечивают высокую пропускную способность.

К сожалению, первоначальная стоимость систем на проксимити-картах выше, чем систем на магнитных картах. Но благодаря отсутствию дополнительных эксплуатационных расходов, стоимость проксимити-систем при длительных сроках эксплуатации оказывается не выше, чем систем, использующих другие технологии считывания.

Карты программируются один раз на заводе. Срок службы активных карт – 5 лет, пассивных – практически неограничен.

Внешний вид карты оформляется по желанию заказчика. На поверхность можно нанести логотип фирмы, имя, фамилию и фотографию пользователя – тогда карточка может одновременно, служить постоянным пропуском.

Температурный диапазон эксплуатации всех моделей проксимити-карт от –25° до +65° С (для автомобильных вариантов от –45° С).

Основные производители оборудования для проксимити-систем – американские фирмы "HID Corporation" ("Hughes Identification Devices"), "Indala Corporation", входящая в компанию "Motorola" и т.д.

Среди параметров, по которым можно оценивать качество систем управления доступом, можно назвать следующие: уровень секретности, пропускная способность, максимальное количество посетителей, вандалозащищенность, способность работы в неблагоприятных условиях, надежность, удобство монтажа, стоимость. Очевидно, что в настоящее время наилучшее сочетание этих характеристик имеют бесконтактные системы доступа, использующие проксимити-жетоны.

Вряд ли можно указать фирму, которая бы предлагала более широкий спектр проксимити-жетонов, чем фирма «Impro Technologies» (ЮАР). Пользователь имеет возможность выбрать тот тип жетона, который более всего соответствует его вкусу:

– круглый с прорезями для ремешка от часов, носимый на руке или просто в кармане;

– в виде кредитной карточки, носимой на клипсе;

– каплеобразный, в виде «слезинки», который можно использовать как брелок;

– в виде плоской кредитной карточки – с прорезями или без них;

– в виде кредитной карточки с магнитной полосой;

– в виде карточки с встроенной клавиатурой (что дополнительно повышает секретность системы, даже в базовом варианте обеспечивающей 94 миллиарда комбинаций).

Указанные жетоны могут использоваться для разрешения прохода в офисах, квартирах, дачах, оснащенных самыми различными приборами фирмы «Impro Technologies» (удобно: всего один жетон вместо связки ключей, оттягивающей карман!).

Следует также упомянуть о жетонах, используемых для иммобилизаторов автомобилей, жетонов, монтируемых на транспортных средствах, жетонов, предназначенных для открывания ворот.

Все проксимити-считыватели фирмы «HID» имеют трехцветный светодиод и зуммер для индикации срабатывания.

MiniProx – компактный проксимити-считыватель. Расстояние идентификации до 14 см. Размеры 152x43x19,1 мм.

Thin Line II – компактный проксимити-считыватель. Расстояние идентификации до 14 см. Стандартный выход Виганда и ABA (магнитная полоса). Размеры 118x75x12 мм.

ProxPro – проксимити-считыватель, максимальное расстояние считывания 23 см. Трехцветный светодиод и зуммер для индикации срабатывания. Существует модель со встроенной клавиатурой. Имеет стандартный выход виганда или интерфейс RS232. Оборудован датчиком вскрытия корпуса. Размеры 127x127x25,4 мм.

MaxiProx – проксимити-считыватель, идентификация на расстоянии до 61 см. Оборудован датчиком вскрытия корпуса для предотвращения попыток взлома. Имеет стандартный виганд-выход. Размеры 305x305x25,4 мм.

ProxCard II – проксимити-карта с прорезью для крепления. Размеры 54x85,7x1,8 мм.

DuoProxТонкая – тонкая проксимити-карта с магнитной полосой (три дорожки ABA стандарта). Размеры 54x85,7x0,9 мм.

PhotoProx – тонкая проксимити-карта со слотом для фотографии. Размеры 54x85,7x1,3 мм.

ISOProx – тонкая проксимити-карта для нанесения фотографии. Размеры 54x85,7x0,9 мм. Модификация ISOProx II – программируемая тонкая проксимити-карта для нанесения фотографии.

ProxCard Plus – тонкая комбинированная проксимити/виганд карта. Размеры 54x85,7x0,9 мм.

ProxKey II – проксимити-брелок. Может программироваться кодом Виганда в диапазоне 26-37 бит. Устойчив к изгибам и ударам. Размеры 48,3x22,9x8,8 мм.

Vehicle ID Tag – пассивная проксимити-метка для учета автотранспорта. Расстояние считывания до 1 м. Гибкая, может крепиться на поверхности неправильной формы (внутри обтекателя на внутренней поверхности лобового стекла). Предназначена для работы со считывателем MaxiProx. Диаметр 99,5 мм. Толщина 2,3 мм. Температура эксплуатации от –45 до +70 °С.

Биометрические терминалы

Насколько бы ни были надежны и удобны проксимити, магнитные или виганд карты, и они имеют недостатки. Главный – карточки можно потерять, забыть дома, в конце концов, их могут просто украсть. Но существует такой "ключ", который человек всегда носит с собой – это он сам, его индивидуальные биологические признаки.

На сегодняшний день перечень выпускаемого оборудования такого типа довольно большой, например – устройства сличения геометрии руки, почерка, рисунка сетчатки глаза, отпечатков пальцев, речевых характеристик и других биологических признаков. К сожалению, эффективность современных биометрических систем еще недостаточно высока, а стоимость довольно велика, поэтому до массового вытеснения других технологий идентификации дело еще не дошло.

Для оценки эффективности различных биометрических систем разработаны специальные методики. Экспериментально определяются численные коэффициенты надежности системы: ошибка первого рода ("ложный отказ" – принятие "своего" за "чужого") и ошибка второго рода ("ложный допуск" – принятие "чужого" за "своего").

Для определения этих параметров необходимы большие массивы статистических данных, для накопления которых порой необходимы многолетние испытания. Значения вероятности ложного отказа и ложного допуска взаимосвязаны: чем больше ошибка первого рода, тем меньше ошибка второго рода, и наоборот. Как правило, производитель дает возможность пользователю самому устанавливать пороги чувствительности и выбирать необходимое соотношение между двумя ошибками.

Кроме этих коэффициентов при выборе типа биометрического терминала следует обращать внимание на следующие факторы:

- уникальность сравниваемых или измеряемых характеристик;
- возможность изменения измеряемых характеристик со временем;
- трудность внедрения системы обработки сравниваемой информации.

Серьезную исследовательскую работу в области систем безопасности, в том числе и биометрических технологий, проводит Сандийская национальная лаборатория (США).

Геометрия руки

Метод биологической идентификации по форме кисти руки был разработан еще в 60-е годы. Первый промышленный аппарат назывался ldentimat и в качестве идентификационного параметра использовал длину пальцев. Рука помещалась на площадку из светочувствительных ячеек, которая освещалась сверху мощной лампой.

В конце 80-х появились современные системы, использующие метод трехмерной идентификации – Hand Key. Этот метод сличения индивидуальных характеристик предусматривает оценку нескольких параметров профиля руки, в том числе ширины ладони и пальцев в различных местах, длины пальцев, толщины и формы пальцев.

Для измерения этих характеристик пользователь помещает руку на панель устройства. Чтобы рука занимала правильное положение, в панель вставлены несколько штырьков-фиксаторов. Для подтверждения корректного расположения руки на панели устройства зажигаются и гаснут четыре светодиода.

Рука освещается инфракрасным светом, а установленная сверху ПЗС-камера регистрирует ее вид. Кроме вида кисти руки сверху в поле зрения камеры оказываются два боковых зеркала, которые дают информацию о толщине ладони. Полученное изображение преобразуется по специальному алгоритму в цифровую информацию, занимающую девять байт. После того как сканирование геометрии руки заканчивается, кодовая информация сличается с эталоном, хранящимся в памяти, и принимается решение о соответствии или несоответствии характеристик. В памяти устройства можно хранить информацию о более чем 10000 пользователях.

Операция снятия, кодирования информации и сверки с базой данных занимает 1-2 секунды.

Процесс первоначальной записи эталона геометрии руки заключается в трехразовом сканировании и усреднении полученной информации. Время первоначальной записи эталона занимает до полутора минут.

Хотя расположение выступов на пластине соответствует конфигурации правой руки, устройство позволяет сканировать и левую руку, обращенную ладонью вверх. Это дает возможность пользоваться системой людям, у которых правая рука повреждена.

Испытания, проведенные Сандийской национальной лабораторией, показали, что частота возникновения ошибки I рода ("ложный отказ") может быть снижена до 0,03 % (при трехразовых попытках удостоверения личности), а частота возникновения ошибки II рода ("ложный допуск") – до 0,1 % (при одноразовых попытках удостоверения личности).

Почерк

Сличение подписей – метод, применяемый в банковском деле уже на протяжении многих десятков лет, несмотря на то, что можно подделать подпись. Защищенность метода значительно повышается, если сравнивать не само изображение подписи, а динамические характеристики процесса подписания. Были разработаны автоматические системы подтверждения почерка, измеряющие характеристики движения руки при письме (усилие нажатия на перо, скорость, ускорение и т.д.). Статистическая оценка этих данных показывает, что подпись обладает рядом уникальных и повторяющихся характеристик. Преобразователи, измеряющие характеристики почерка, могут быть установлены как в пишущем устройстве, так и под пластиной, на которой ставится подпись.

Дактилоскопия

Дактилоскопические исследования (анализ отпечатков пальцев) используются в криминалистике уже более столетия. Сличение отпечатков пальцев считается одним из наиболее надежных способов распознавания индивидуальных характеристик. Отпечатки пальцев (папиллярные узоры) строго индивидуальны и остаются неизменными на протяжении всей жизни.

Одну из самых надежных дактилоскопических систем представляет американская компания "Identix" – Touch Lock . При пользовании системой необходимо набрать свой код на клавиатуре и приложить палец к сканеру папиллярного узора. Считывание и проверка занимают 5-6 секунд.

Ошибка I рода ("ложный отказ") составляет 2%.

Ошибка II рода ("ложный допуск") – 0.0001%.

Терминал Touch Lock можно использовать в сети (до 32 считывателей).

В России из импортных комплектующих собирается дактилоскопическая система Кордон. Время идентификации 2-4 с, время регистрации нового пользователя около 1 мин, математический код отсканированного пальца занимает 0,5 Кбайт.

Ошибка I рода составляет 1%.

Ошибка II рода – 0.0001%.

Рисунок сетчатки глаза

Конфигурация кровеносных сосудов человеческого глаза неповторима, и на этом основана система идентификации по рисунку сетчатки глаза, производимая компанией «Eyedentify Inc.» (Портленд, штат Орегона).

Круглый участок сетчатки, расположенный вокруг центра хрусталика, сканируется неполяризованным светом низкой интенсивности, который испускается инфракрасными светодиодами. Различная интенсивность света, отраженного от разных точек сетчатки в процессе сканирования, отображает индивидуальное расположение кровеносных сосудов.

При сканировании рисунка сетчатки глаза служащий должен неподвижно смотреть на светящуюся точку в видоискателе устройства. Обычно, для более точного определить расположения кровеносных сосудов регистрация рисунка сетчатки производится несколько раз подряд.

Идентификация – подтверждение введенного с клавиатуры PIN-кода – требует только одного сканирования, и вместе с процессом сравнения с базой данных занимает до 7 секунд. Устройство идентификации рисунка сетчатки глаза фирмы «Eyedentify Inc.», в отличие от системы других компаний, может работать в режиме «распознавания», не требующем ввода PIN-кода. В процессе проверки просматривается информация о сетчатках всех служащих со скоростью сличения 100 эталонов в секунду.

Данные, полученные при испытаниях в лабораторных условиях, показывают, что частота возникновения ошибки I рода (ложное отрицание сходства) составляет для таких устройств 0,4%, а частота возникновения ошибки II рода (ложное подтверждение сходства) – 0%.

Система идентификации по рисунку сетчатки глаза – одна из самых надежных, но ее распространение связано с трудностями психологического характера. Некоторые люди, особенно женщины, крайне болезненно относятся к процедуре и отказываются смотреть на яркий луч света. По данным ряда социологов, 4% сотрудников не согласны пройти процедуру сканирования сетчатки. Хотя, по утверждению медиков, эта процедура полностью безопасна.

Но, несмотря на все недостатки, аналогичные системы уже достаточно распространены. Например, в середине 1997 года ведущий производитель банкоматов компания «Сенсар» заключила соглашение с американской фирмой «NCR Corp.» об установке в новые банкоматы специальных телекамер для определения оттенков радужной оболочки. Интересно, что идентификация происходит на расстоянии 3 фута (почти метр).

Характеристика речи

Определение характеристик речи – один из развивающихся методов идентификации. В число измеряемых характеристик речи, улавливаемой микрофоном, входят:

- огибающая формы сигнала;
- период высоты тона;
- относительный спектр амплитуды;
- резонансные частоты речевого тракта (форманты).

Основное применение: доступ к компьютерным сетям по телефону Несколько устройств распознавания характеристик речи выпускаются для систем пропускного контроля. Ведутся активные дальнейшие разработки в этой области. В качестве существенных проблем, с которыми пока плохо борется современная техника, можно отметить: влияние на качество идентификации посторонних шумов и сложность в борьбе с изменениями тональности (насморк, настроение и т.д.). Кроме этого, существенным оказывается психологический фактор: если система хотя бы один раз не пропустила пользователя, то человек, помня о неудаче, начинает волноваться, старается подстроить голос, в результате шансов на идентификацию у него становиться еще меньше. Представьте себе, что вас заблокировали в тамбуре безопасности.

Инфракрасная технология распознавания лица

Лицо каждого человека имеет свою индивидуальную тепловую карту, которая зависит от характеристик сосудистой системы и ряда других физиологических характеристик и не меняется с возрастом и состоянием здоровья. Тепловой образ лица – это своего рода комбинация термальных свойств сосудистых структур, их формы и плотности, свойств подкожных тканей, хрящей, кожи и т.д. Даже у близнецов тепловые карты лица различны. Более того, если верить производителю, тепловая карта лица остается прежней после пластической операции. Поэтому существует возможность производить пассивное, независящее от освещенности и небольших вариаций температуры окружающей среды, распознавание пользователей системы на основе инфракрасных характеристик их лиц.

Эту возможность успешно реализовала американская компания «Technology Recognition Systems». В основе системы – ИК-камера, которая снимает тепловую карту лица. Сигнал, полученный с камеры, обрабатывается компьютером по специальному алгоритму.

Другие методы подтверждения индивидуальных характеристик

Изучались и другие методы подтверждения индивидуальных физических характеристик. Например, методы, основанные на использовании электрокардиограмм, характеристик походки и т. д., но в этих направлениях не было создано серьезных промышленных разработок.

Персональный идентификационный номер, клавиатура

Идентификационную карточку можно украсть. В этом, к сожалению, главный недостаток многих систем управления доступом за исключением, конечно, биометрии. Поэтому вместе со считывателями на дверь иногда дополнительно ставится специальная цифровая клавиатура. В этом случае пользователь кроме считывания карты должен еще набрать на панели известный только ему и оператору системы персональный идентификационный номер (PIN).

Для обеспечения повышенной безопасности некоторые производители даже выпускают виганд, проксимити или другие считыватели со встроенной клавиатурой.

Иногда клавиатуру применяют без каких-либо считывателей. Тогда система получается достаточно дешевой, но слабо защищенной от взлома, т. к. цифровой код достаточно просто подсмотреть. Для большей защиты коды регулярно меняют. Но при этом резко возрастает число случаев, когда пользователи забывают код.

Для исключения возможности подсматривания набираемого кода американская фирма «Hirsch» разработала особую клавиатуру ScramblePad. Она содержит сразу несколько оригинальных технических решений. Во-первых, клавиатура устроена так, что при каждом включении расположение цифр на панели принимает случайный порядок. Во-вторых, угол, в пределах которого видны светящиеся цифры, ограничен. Например, клавиатура модели DS37L

имеет угол обзора 26 град. по вертикали и 4 по горизонтали. Разглядеть, какой код набирает сотрудник, практически невозможно. Поэтому, даже если злоумышленник запомнит, какие клавиши нажимал пользователь, при повторе той же комбинации у него ничего не получится.

Достоинством клавиатур доступа является их низкая стоимость – например, клавиатура FC21E итальянской фирмы «Farfisa» стоит всего $29. Естественно, если требуется вандалозащищенное исполнение клавиатуры (например, итальянской фирмы «Videx» или испанской фирмы «Fermax»), то такой прибор стоит несколько дороже.

Общим для всех клавиатур является то, что для повышения секретности они допускают вхождение в режим программирования с целью изменения кода доступа. А отличием клавиатур друг от друга является то, что для вхождения в этот самый режим в одних приборах достаточно нажать микрокнопку на задней панели (аппаратный способ), а в других для этого нужно с клавиатуры ввести мастер-код (программный способ). Так вот, все дело в том, что в клавиатурах второго типа (например, «Videx») сразу после вхождения в режим программирования в первую очередь следует подтвердить старый, либо установить новый мастер-код. Если об этом забывают, в дальнейшем уже войти в режим программирования, увы, не удастся.

Но если подобное случится с Вами, не спешите отчаиваться и не тратьте лишних денег на ремонт клавиатуры. Это «лечится» очень просто: выключите питание, нажмите ENTER и, удерживая данную кнопку, включите питание – прибор вернется к заводским установкам.

2.6. Преобразователи кодов

Допустим, вы решили приобрести удобный проксимити-считыватель, который хорошо впишется в интерьер вашего офиса. Как его подключить к уже установленной на объекте СУД? Скорее всего, считыватели и контроллеры различных производителей не совместимы напрямую.

Когда СУД стали широко распространенными, серьезно встала проблема совместимости считывателей и контроллеров разных производителей. Оказалось, что аналогичные считыватели разных торговых марок не всегда взаимозаменяемы. Поэтому была предпринята попытка ввести хоть какое-то единообразие. В частности, производители договорились, что контроллер и считыватели должны быть связаны единообразным 26-битным виганд-интерфейсом.

Но время течет, потребности меняются, увеличиваются массивы передаваемых данных и 26 бит не всегда хватает. Сегодня кроме 26-ти еще используются 32-, 34- и 48- битные интерфейсы.

Каждый производитель находит свои «тропинки» взаимодействия с оборудованием других производителей. Самое популярное решение – использование так называемых преобразователей кодов. Инженеры разрабатывают плату, которая ставится между контроллером и считывателем. Задача платы – получать на входе сигнал по интерфейсу считывателя и выдавать информацию контроллеру по стандартному для него интерфейсу. Преобразователь

кода – это буфер, который предназначен для перевода информации в понятный для контроллера вид.

Как правило, преобразователь кода – это плата с размещенными на ней микропроцессором, ПЗУ, переключателями, перемычками и т. д. Когда возникнет необходимость подсоединить тот или иной считыватель, пользователь системы открывает инструкцию по эксплуатации, ищет схему, соответствующую данному типу интерфейса, и переставляет перемычки согласно схеме. К примеру, так работает плата Match американской компании «Hirsch».

Кроме этого, есть программные преобразователи кода. Например, для настройки системы фирмы «Software House» (США) на определенный тип считывателя не переставляют перемычки на плате, а программируют интерфейс.

2.7. Исполнительные устройства

Зачастую при проектировании системы безопасности исполнительным устройствам (замкам, турникетам, доводчикам, кнопкам выхода и т.д.) не уделяется должного внимания. Иногда на этом даже пытаются экономить, что крайне недальновидно. Необходимо помнить, что исполнительные устройства постоянно работают в физическом контакте с другими элементами, поэтому наиболее сильно подвержены износу. Хороший замок выдерживает до миллиона срабатываний. Опыт показывает, что наибольшее число отказов системы происходит именно из-за недостаточно серьезного подхода к выбору исполнительных устройств. Сэкономленная на исполнительных устройствах сотня долларов может поставить под вопрос эффективность всей системы стоимостью десятки тысяч долларов.

2.7.1. Замки

Замок – достаточно древнее изобретение. Еще в Древней Греции были распространены замки с гребенкой, закрепленной на внутренней стороне двери. Открывались же эти замки «ломающимся» коленчатым ключом, который зацеплялся за гребенку и передвигал ее.

Первые навесные замки появились в Китае, а оттуда через Индию разошлись по всему миру.

В России в X веке были изобретены навесные пружинные замки со съемной дужкой. Дужка имела на конце два пружинных захвата. Когда ее вставляли в корпус замка, захваты расходились и удерживали ее в корпусе. Открывался замок ключом в виде лопаточки с отверстием. Ключ вводился в замочную скважину, надевался на конец дужки с захватами, захваты стягивались и дужка освобождалась, открывая замок. Эти замки вывозились из России в Европу и там назывались «русскими».

Напомним, что по типу крепления замки подразделяются на врезные, накладные и навесные, по принципу действия – на механические, электроме-

ханические (соленоидного, моторного и куркового типов), электромагнитные и др.

Говоря об электрических замках, используют термины – «нормально открытый» и «нормально закрытый». «Нормально открытый» означает, что замок без напряжения находится в открытом состоянии, а «нормально закрытый» замок без подачи питания находится в закрытом состоянии. «Нормально открытые» замки очень нравятся пожарным инспекторам, т.к. в случае пожара и отключения питания дверь автоматически разблокируется, что может быть принципиально важным при эвакуации. А представители службы безопасности, как правило, предпочитают нормально закрытые замки, т.к. даже при отключении питания дверь остается закрытой.

2.7.2. Датчики состояния двери

Для определения положения двери (закрыта она или открыта) существуют специальные дверные магнитоконтактные датчики или герконы (герметичные контакты). По типу крепления датчики бывают врезные и накладные. Герконы имеют две части, которые крепятся на двери и на дверной коробке. Необходимо помнить, что при установке датчиков на дверь вместе с электромагнитным замком, надо разнести замок и геркон как можно дальше.

На части замков «Abloy» есть специальные датчики (микропереключатели), которые устанавливаются на ответную пластину и определяют положение ригеля.

Недорогой геркон можно отключить с использованием достаточно сильного магнитного поля. Поэтому на особо важных объектах применяют более дорогие, но и более надежные магнитостабилизированные контакты, защищенные от влияния внешнего электромагнитного поля.

Кроме герконов и микропереключателей существует еще целая масса датчиков, использующих различные физические явления (инфракрасные, емкостные и т. д.). Все модели датчиков состояния двери имеют на выходе сухие контакты и подключаются к элементам системы, контролирующей ту или иную дверь.

В ряде случаев, использование датчиков состояния обязательно, например с электрическими замками, имеющими один ригель прямой конструкции. Датчик состояния определит, когда дверь открыта, и даст сигнал убрать ригель в корпус замка.

2.7.3. Двери, кабелепроводы

При оборудовании объекта в наиболее ответственных местах рекомендуется использовать только стальные двери.

Если все же по каким-то причинам необходимо оставить деревянную дверь, то ее следует укрепить: во-первых, усилить дверную коробку, а во-вторых, поставить распорные замки или замки типа «балка». Распорный замок закрывает дверь в нескольких местах сразу, а замок типа «балка» пред-

ставляет собой металлическую балку, которая накладывается во всю ширину двери.

На стальные двери лучше всего поставить два разных замка. Например, один – удобный в обращении механический цилиндровый, электромагнитный или электромеханический, а другой – для надежности (сувальдный, электромоторный, соленоид или др.). У монтажников принято делить устанавливаемые замки на «дневные» (удобные в эксплуатации, быстрые, выдерживающие большие нагрузки – до 500-1000 проходов в день) и «ночные» (более надежные, устойчивые к взлому, но выдерживающие небольшое число проходов – 50-100 тысяч за весь срок эксплуатации).

Красивые электрические замки требуют подведения электропитания. Для этого вдоль двери сверлят отверстие, по которому проводят кабель, а для передачи кабеля из дверной коробки в дверь используют специальные кабелепроводы. Это приспособление состоит из гофрированной трубки, через которую пропускается кабель, и желоба, устанавливаемого в дверь, в который помещается трубка при закрытии двери.

Достаточно интересные модели накладных замков для стеклянных дверей предлагает петербургская компания «ПЭРКо». Питание к замку подается не через корпус, как обычно, а через ригель. В нормальном состоянии замок закрыт и ригель соприкасается с контактами на ответной части, вмонтированной в дверной косяк. Когда на замок подадут напряжение, он взведется, дверь откроется. При закрытии двери срабатывает собачка, и замок просто защелкивается.

И еще одна деталь, о которой часто забывают при проектировании системы. Поблизости от двери с внутренней стороны необходимо установить кнопку экстренной разблокировки двери. Кнопка должна стоять на видном месте под стеклом, аналогично кнопке пожарной тревоги. Тогда в случае пожара или, скажем, землетрясения проход будет оперативно разблокирован.

2.7.4. Доводчики

Допустим, вы поставили хорошие замки, считыватели, укрепили двери. Но вся польза от этого может быть сведена на нет, когда на двери нет доводчика. Если какой-то забывчивый сотрудник не захлопнет дверь после своего прохода, то это за него сделает доводчик. Доводчики бывают самые разные: от простых отечественных или импортных, до мощных программируемых систем.

Дешевые доводчики широко распространены и есть практически в каждом офисе, магазине, гостинице (например, в Москве достаточно часто можно встретить модели фирм «CISA» (Италия), «Yale» (США), «Dorma» (Германия) и др.). А вот среди дорогих моделей встречаются очень интересные образцы.

Функция доводчика – не только гарантировать закрытие двери, он еще должен оберегать замок от механических ударов, а при пожаре автоматически раскрывать двери и помогать эвакуации. Некоторые модели доводчиков

имеют, так называемую «систему торможения с подтягом» – вначале доводчик дает двери разогнаться, потом тормозит движение и уже в конце, у самой двери, резко подтягивает дверь, обеспечивая гарантированное закрытие.

Есть очень интересные разновидности доводчиков – электроприводы распашной двери, например, модель «Abloy» 830, которая имеет микропроцессорное управление и по сути является автономным комплексом управления дверью. Эта модель – что-то вроде умного и заботливого электронного швейцара. Для того чтобы случайно не придавить руку посетителя или, скажем, кошку, доводчик имеет встроенный режим безопасности – при возникновении препятствия в момент закрывания, дверь автоматически откроется. Электропривод может соединяться с элементами системы безопасности: кнопками выхода, фотоэлементами, считывателями, замками. Им можно управлять дистанционно, например, из-за бронированной кабины на проходной. Максимальное толкающее усилие 230 кг, максимальное втягивающее – 160 кг.

2.7.5. Шлюзы

Перед службами безопасности всех более или менее важных объектов, как правило, встают одинаковые задачи: как защитить вход от вооруженного штурма, как блокировать нарушителя, как не допустить пронос на объект оружия, взрывчатки и отравляющих веществ, как выделить из общего потока персоны с особыми полномочиями и обеспечить их быстрый и беспрепятственный проход и т.д.

Львиную долю этих проблем можно решить, организовав специальные тамбуры безопасности (шлюзы). Основная задача тамбура – разделить людской поток на отдельных людей, изолировать посетителя в особом помещении, где при необходимости можно произвести его идентификацию и обследовать на предмет наличия запрещенных к проносу предметов, а в случае чего и заблокировать до прибытия милиции.

Шлюз – это специальный комплекс из двух взаимосвязанных дверей, созданный для раздельного прохода. Непременное условие функционирования шлюза – дверь на выход откроется только в том случае, если входная дверь блокирована и сотрудник обладает правом прохода. Как правило, шлюз оснащается устройствами идентификации, расположенными перед входом или внутри шлюза. В целях повышения безопасности нередко шлюзы дополнительно оборудуются:

- детекторами металла для обнаружения у посетителей оружия и т.д.;
- рентгеновскими аппаратами для досмотра личных вещей;
- датчиками взрывных и отравляющих веществ;
- системой взвешивания для обнаружения забытых вещей и попыток прохода вдвоем.

Кроме всего прочего, датчики идентификации личности позволяют выделять из потока посетителей персоны, наделенные особыми полномочиями.

Для лиц, имеющих право проноса оружия и право прохода без досмотра, изменяется алгоритм работы шлюза.

Схем строения шлюзов достаточно много. В качестве материалов используют как обычные, так и огнестойкие и пуленепробиваемые стекла, пластики, сталь или алюминий.

При проектировании системы безопасности необходимо предусмотреть варианты работы системы в случае возникновения пожара или угрозы террористического акта. Для свободного выхода персонала при эвакуации в комплексе со шлюзом устанавливают дверь, заблокированную в обычном состоянии, но в экстренных случаях автоматически открывающуюся и пропускающую большие потоки людей.

Пропускная способность шлюзов – 5-10 человек в минуту. Конечно, эта цифра приблизительна и сильно зависит от числа приложений (наличия всевозможных детекторов и т.п.).

Производители, вышедшие на российский рынок – «Erapa» (Швейцария), «Secod Italia», «Blindart Pomezia», «Nuova Vetro» и «Saima» (Италия), «Schneebeli» (Германия) и т. д.

2.7.6. Турникеты в полный рост

Внешне эти турникеты похожи на обычные «трехлистные» двери, но для запрещения прохода в обратном направлении они оснащены ограждениями. Положение ротора фиксируются специальной замковой системой, соединенной с пультом управления или считывателями.

К сожалению, габариты, специально рассчитанные на проход только одного человека, создают трудности для тучных людей, которым порой непросто протиснутся в стандартизованные проходы. Кроме того, при проектировании проходной необходимо обязательно предусмотреть возможность прохода человека на инвалидной коляске или проноса крупногабаритных вещей.

Выпускаемые турникеты различаются как дизайном, так и материалом, из которого они изготовлены.

Для работы в уличных системах рекомендуется использовать турникеты из нержавеющей стали или с защитным покрытием (например, с гальваническим). Такие модели легко встраиваются в ограду и надежно защищают места прохода (модель STG фирмы «Burle», модели серии full-o-stile фирмы «Italdis Industria», THT-100 «Tomsed Corporation» и т.д.).

Для применения внутри помещений более целесообразно использовать турникеты из алюминия. Конечно, они уступают стальным по прочностным характеристикам, но зато более элегантны и почти не требуют усилий для прокрутки.

Кроме того, есть модели турникетов, лепестки которых выполнены из прозрачного пластика (например, CSTG «Burle»). Эти модели облегчают визуальный контроль за входящими и позволяют более эффективно использовать телекамеры, следящие за входом.

2.7.7. Поясные турникеты

Поясной турникет – устройство высотой 120-150 см. Обычно устанавливается на проходных. Главный недостаток – невысокая степень физической защиты. При желании турникет можно перепрыгнуть. Поэтому основное применение – элемент системы учета рабочего времени. Существует несколько типов поясных турникетов:

– вращающийся (наиболее распространенный тип);
– сдвижной (такой турникет установлен в Московском метро);
– распашной (другое название – электромеханическая калитка). Калитка внешне напоминает прозрачную дверь, как правило, в половину обычной высоты.

Турникеты могут дополнительно оснащаться:

- счетчиками проходов;
- устройствами освобождения прохода в случае эвакуации;
- светодиодными индикаторами состояния;
- устройствами для дистанционного управления турникетами;
- считывателями различных технологий;
- специальными регистрирующими датчиками для фиксации и предупреждения попыток перепрыгивания и подлезания.

Турникеты могут позволять проходить в двух направлениях или только в одну сторону. Но в любом случае он имеет систему фиксации, не позволяющую человеку после начала движения развернуться и пойти в обратную сторону.

Конструкция турникета должна гарантировать невозможность одновременного прохода двух человек.

Наиболее распространены в России турникеты компаний «Italdis Industria» и «Mayor», входящих в шведский концерн «Gunnebo», американской фирмы «Tomsed Corporation» и российской «ПЭРКо». «Italdis Industria» производят весь спектр турникетов: с вращающимися брусьями серии turn-o-mat, universal и sentinell, с раздвижными/складывающимися створками серии hidden gate и др. Стоимость трехштанговых турникетов колеблется от 3 до 10 тысяч долларов, в зависимости от модели и дополнительных модулей. Турникеты серии hidden gate более дорогие, но в отличие от турникетов с вращающимися брусьями, эти турникеты гарантируют более высокий уровень безопасности. Они могут работать как в «нормально открытом», так и в «нормально закрытом» режимах. При работе в «нормально открытом» режиме турникет всегда открыт. При подходе человека срабатывает детектор движения и система идентификации. Если человек не имеет право прохода, то створки закроются, если имеет, то соответственно нет. Длина этих турникетов 1,5 м, а высота стеклянных створок до 1,7 м.

Большинство турникетов спроектированы на максимальную пропускную способность до 60 человек в минуту. Но это расчетные данные. На практике же пропускная способность турникета в тандеме с расторопным вахте-

ром максимум 30 человек в минуту. А при использовании электронных систем управления доступа эта цифра снижается до 15 человек в минуту. Для случаев, когда необходимо пропускать большее число людей в минуту, выпускают сдвоенные версии турникетов. Естественно, они дешевле и компактнее, чем два одинарных.

2.8. Программное обеспечение

Системы управления доступом базируются на самых современных достижениях науки и техники. Основа большинства СУД – мощная микропроцессорная техника, без которой невозможно обработать колоссальные объемы информации. Поэтому программное обеспечение играет очень большую роль. Крупные многодверные системы без ПК и программного обеспечения (ПО) просто не смогут полноценно функционировать.

2.8.1. Состав ПО

Из-за большой гибкости программного обеспечения, продукция различных фирм сильно отличается друг от друга. Поэтому составить общее описание ПО разных производителей задача достаточно сложная.

Вообще говоря, рассматривая программное обеспечение, можно выделить ряд подпрограмм:

- программы настройки и управления системой;
- модуль системной интеграции;
- программы печати на карты и выброса на монитор фотографии пользователя;
- программы алармовой (тревожной) графики и мониторинга событий.

2.8.2. Функции ПО

Программное обеспечение призвано обеспечивать следующие функции:

- ввод данных идентификационных устройств в базу данных
- задание характеристик пунктов доступа;
- задание временных групп;
- задание уровней доступа;
- программная поддержка взаимодействия элементов различных систем;
- обновление и хранение базы данных;
- мониторинг и протоколирование текущих событий и т.д.

2.8.3. Программирование СУД

Программирование системы начинается с задания пунктов доступа. Под пунктом доступа понимают физическое место, где осуществляется доступ. Пунктом доступа может быть дверь, шлюз, турникет. Пункты доступа оборудуются считывателями, исполнительными устройствами и т.д. При этом обычно вводятся следующие данные: название и параметры считывателя, его

системный адрес, время открывания замка, реакция системы на нажатие кнопки выхода, на взлом двери, на удержание двери в открытом состоянии, использование считывателя в режиме antipassback и для учета рабочего времени, режим отслеживания карт, возможность ручного управления пунктом доступа и т.п. Если пункт доступа оснащен дополнительно клавиатурой, то вводится тип клавиатуры, время, в течение которого клавиатура отключена (вход только по карте), использование дополнительного выхода и методы его переключения.

Как правило, рабочий день в любом банке, компании или предприятии строго регламентирован (например, с 9.00 до 18.00). Но есть обслуживающий персонал – уборщицы, повара, сторожа и др., которые работают в иные часы. Но при этом, подавляющая часть работников не должна приходить раньше положенного времени. Для разделения права доступа по времени все сотрудники, от директора до уборщицы, разбиваются на группы, имеющие право входа в строго регламентированные временные промежутки. Например, уборщицы могут входить с 7.00 до 10.00, клерки с 9.00 до 18.00, управляющий с 7.00 до 22.00 и т.д.

Программируя базу данных, администратор вводит информацию о каждом пользователе. Вводимые данные можно условно разделить на две части: системные данные и частная информация. Под системными данными понимают обязательную информацию о пользователе: номер карты, уровень доступа, код для ввода с клавиатуры, время действия карты. Частные данные заносятся администратором системы в более свободной форме. Как правило, в систему вводят фамилию, имя, отчество пользователя, подразделение, должность и т.д.

По базе данных можно производить поиск информации, например по номеру карты, по фамилии и т.д.

Для каждой карты индивидуально может быть задан срок действия. При нарушении сроков действия карты система запрещает автоматический проход и выдает соответствующее сообщение на компьютер.

Функция локализации и учета пользователей позволяет в любое время определять количество пользователей в заданном помещении. Это крайне важно в аварийной ситуации, когда нужно оперативно установить, где находятся сотрудники. Кроме того, функция позволяет организовать систему учета рабочего времени, предоставляющую информацию о количестве часов, проведенных каждым сотрудником на рабочем месте.

Для каждого считывающего устройства задаются все касающиеся его данные. Для наглядности считывателю можно дать название, например «Главный вход» или «Проходная № 2».

Внутри системы можно формировать и выводить на монитор или принтер различные отчеты и сводки.

В любой момент можно сделать запрос о состоянии каждого пункта доступа. Используя эту же функцию, можно, например, не покидая поста контроля, открывать ворота (это очень удобно, например, при приеме груза).

Подсистема управления тревожной сигнализацией позволяет формировать охраняемые зоны, которые независимо друг от друга ставятся в состоя-

ние «активировано» или «покой». Несколько различных зон можно объединить в сектор, сигнал тревоги от которого может быть использован для управления работой телевизионных камер. Это позволит фиксировать на видеопленку случаи нарушения режима допуска на объекте.

Налаживание взаимодействия СУД с другими системами безопасности, как правило, заключается в программировании логических цепочек: событие – условие – действие.

В качестве событий могут выступать считывание карты, на разрешение режима доступа, срабатывание датчика сигнализации или видеодетектора движения и т.д.

Все происходящие события пропускаются системой через маску условий. Если, например, один из считывателей системы управления доступом идентифицировал пользователя, то система проверит соответствие события временным рамкам, проверит наличие у пользователя права доступа и т.д.

Если произошедшее событие удовлетворяет поставленным условиям, то в результате система выполнит какое-то заранее запрограммированное действие, например инициализирует общую тревогу, блокирует дверь и т.д.

Программы печати на карты и выброса на монитор фотографии пользователя дают возможность работать с базой фотографий пользователей.

Хотя фотоизображения посетителей занимают достаточно большие объемы памяти, есть ряд приложений, для которых необходима база пользователей, включающая их фотоизображения. Это – и станции печати на карты-пропуска, и программа автоматического вывода на монитор фотографии владельца карты при ее считывании, и ряд других более экзотических приложений.

Информация о пользователе, включая его фотографию, может быть нанесена на любую карту-идентификатор, используемую в системах управления доступом (магнитную, виганд, проксимити и т.д.). Для этого разработано большое число различных устройств печати на карты, использующих сублимационную и термотрансферную печать.

Принтеры позволяют не только наносить изображение на карту, но и одновременно кодировать магнитные полосы, программировать смарт-карты, наносить высококачественные штрих-коды. В ряде случаев, когда печать непосредственно на карты затруднительна (например, для активных проксимити-карт, которые имеют пластиковый корпус, не выдерживающий перегрев), изображение наносится на специальную самоклеющуюся пленку, которая в свою очередь наклеивается на карту.

Кроме того, разрабатывать и выводить на печать макет карты можно и при помощи обычных широко распространенных программ, например CorelDraw. В комплекте с принтером поставляются драйверы для ОС Windows и Interface Kit for Macintosh.

Обслуживать принтер предельно просто. В него закладываются заготовки и через 20-80 секунд получается качественная полноцветная карта с разрешением, как было уже замечено, 300 точек на дюйм. Самые серьезные различия между принтерами заключаются в удобстве печати, в возможности или невозможности одновременного программирования магнитной полосы, нане-

сения поверх краски ламинирующего покрытия и в размерах полей печати. Многие принтеры позволяют печатать на всей поверхности карты, но ряд моделей требуют полей (по несколько мм от края).

В России наиболее распространены принтеры серии Persona (фирма «Fargo», США), Magicard («Ultra Electronics», Великобритания), серии P3OO и P400 («Eitron», США и «Privilege», Франция), ImageCard («DataCard», США) и т.д.

При оборудовании контрольно-пропускного пункта нередко используют интересную и порой крайне необходимую программу. Суть ее работы в следующем. При подходе пользователя к турникету или к входной двери устройство идентификации, установленное на входе, считывает с идентификационной карты код пользователя. По этому коду в базе данных находится информация о пользователе, на имя которого зафиксирована считанная карта. Эти данные, включая и фотографию пользователя, выводятся на монитор компьютера охранника, сидящего за пуленепробиваемым стеклом. Посмотрев на монитор и сравнив фото на мониторе с человеком, подошедшим к турникету, охранник подтверждает или не подтверждает право на проход и разблокирует или не разблокирует турникет.

Программы алармовой (тревожной) графики и мониторинга событий устанавливаются на посту охраны. Они позволяют оперативно в режиме реального времени отслеживать ситуацию на объекте, а в случае тревоги быстро оценивать обстановку и своевременно принимать адекватные меры.

Оператор системы в графическом редакторе (в простейшем случае в CorelDraw) рисует поэтажные планы объекта. Потом переводит эти планы в программу алармовой графики и наносит на них при помощи условных стандартных значков элементы систем безопасности. В качестве обозначаемых элементов часто используют двери, взятые под охрану, датчики сигнализации, телевизионные камеры.

При появлении тревоги программа автоматически выводит на монитор план этажа и выделяет на плане место, откуда поступило тревожное сообщение. Используя протокол событий или задействовав какие-то другие средства (например, охранное телевидение), можно оперативно выяснить, что произошло.

На системном мониторе оператора в реальном масштабе времени отображаются все события, происходящие с системой (например, доступ пользователю разрешен, отказ в доступе и т.д.). Все тревожные события выделяются цветом и сопровождаются звуковым сигналом.

Программное обеспечение должно быть устойчиво к случайным и преднамеренным сбоям в работе, как то: отключение компьютера, программный или аппаратный сброс компьютера и т.д. Если указанные неприятности произойдут, система должна сохранять работоспособность и текущие установки. При выходе компьютера из строя не должно происходить открывания заграждающих устройств.

3. СИСТЕМЫ ОХРАННОЙ И ПОЖАРНОЙ СИГНАЛИЗАЦИИ

Системы охранной и пожарной сигнализации (ОПС) относятся к средствам обнаружения угроз и считаются основными средствами защиты объекта. Система ОПС объекта должна быть эффективной и срабатывать своевременно. Своевременность срабатывания подразумевает обнаружение угрозы на том этапе, когда у службы охраны достаточно времени и сил для ее (угрозы) ликвидации. Эффективность системы защиты может быть оценена по времени с момента возникновения угрозы до ее ликвидации. Чем это время меньше, тем эффективнее система защиты. Важным системным параметром является вероятность ложного срабатывания сигнализации. При проектировании надо добиваться минимума ложных срабатываний при 100% регистрации проникновений. Оптимальной же системой защиты можно считать такую, наличие которой блокирует даже появление мыслей о нападении на защищаемый объект.

Система ОПС, как правило, состоит из следующих частей:

- датчиков (сенсоров, извещателей);
- каналов связи между частями системы;
- приемно-контрольного прибора;
- светового и звукового оповещателей;
- источников электропитания компонентов системы.

Все компоненты приведенной структуры могут быть представлены в реальной системе ОПС как буквально, так и в различных конструктивных комбинациях вплоть до вырожденного варианта автономного пожарного дымового датчика, в котором совмещены и сенсор, и схема обработки с блоком питания, и светозвуковой сигнализатор. Аналитическая классификация компонентов системы без привязки к выполняемой задаче имеет несколько формальный характер. Это надо помнить при подходе к проектированию системы с точки зрения оптимальной функциональной реализации.

В техническом задании на разработку системы охранной сигнализации должно быть указано:

1. Количество помещений, подлежащих блокировке, с указанием типа, количества и местоположения сигнализационных датчиков (возможен другой подход – не указывать тип и количество датчиков, а задавать надежность регистрации нарушителя с указанием способов проникновения, и вероятность ложных тревог).

2. Распределение охраняемых помещений по сигнальным шлейфам (зонам), имеющим порядковый номер и систему их нумерации, в привязке к планам этажей. Присвоение каждому шлейфу вида сигнала тревоги при срабатывании и других эксплуатационных параметров (задержка срабатывания на вход и на выход, способ снятия и постановки на охрану и пр.).

4. Количество и местоположение центрального и местных пультов охраны, блоков управления сигнализацией, тревожных оповещателей.

5. Трасса и способ прокладки коммуникаций.

6. Основной и резервные источники энергоснабжения.

7. Способ отображения оперативной информации (экран компьютера, световое табло и т.д.).

8. Порядок и иерархия полномочий при снятии и постановке зон на охрану и снятия с охраны.

9. Система регистрации и накопления служебной информации в процессе работы системы (фиксация даты, времени срабатывания датчиков и снятия сигналов тревоги, самодиагностика работоспособности аппаратуры и коммуникаций, количество событий, которое должно удерживаться в памяти системы).

10.Способы взаимодействия с системами контроля доступа и телевизионного наблюдения.

Кроме того, в системе сигнализации должны быть обеспечены:

- гибкое модульное построение блок-схемы системы;
- возможность программирования режимов работы, типов зон, количества регистрируемых событий;
- защиту от статического электричества, атмосферных разрядов и других воздействий среды;
- помехозащищенное соединение всех блоков системы;
- возможность вывода части функций по управлению системой из-под контроля дежурного охранника;
- невозможность скрыть факты срабатывания сигнализационных датчиков дежурным охранником (оператором);
- регистрацию и сохранение в памяти всех эксплуатационных событий (отключение сети электропитания, неисправность отдельных блоков, снятие и постановку на охрану, продолжительность тревожного сигнала и пр.) с указанием времени и даты события;
- защиту от попыток нейтрализации системы сигнализации в рабочем и отключенном состоянии.

3.1. Датчики ОПС

Важнейшими компонентами ОПС по праву считаются датчики (сенсоры, извещатели). В общем случае они выдают сигнал об изменении параметров окружающей их среды. Классифицировать датчики можно по самым различным параметрам:

1) по месту установки на объекте:

- внешние (за пределами здания);
- внутренние (внутри помещения).

2) по способу установки:

- скрыто установленные;
- открыто установленные.

3) по типу энергопитания:

- не требующие питания;

- автономные (со встроенным источником питания, либо питающиеся от среды, либо с локальным сетевым источником);
- получающие питание от приемно-контрольного прибора:
  - а) по отдельным проводным линиям;
  - б) по информационным линиям.

4) по принципам сигнализирования о происшедшем событии:

- замыкание или размыкание "сухих" контактов реле;
- изменение потребляемого тока (проводимости);
- передача кодированного сигнала в линию или в эфир.

5) по принципам взаимодействия со средой:

- пассивные – принимают и обрабатывают сигналы, поступающие из среды без инициирующего воздействия на нее;
- активные – излучают в среду сигнал и следят за его изменениями.

6) по конструктивным характеристикам:

- локальной установки;
- распределенные.

7) по физическим принципам:

- магнито-контактные (герконовые);
- инфракрасные (пассивные и активные);
- микроволновые (СВЧ);
- ультразвуковые;
- сейсмические;
- электроконтактные (обрывные, натяжные, нажимные, вибрационные и т.п.);
- емкостные (индуктивные);
- кабельные;
- видеосигнальные;
- микрофонные;
- фотоэлектрические;
- поршневые (" subsonic – effect");
- радиоактивные (радиоизотопные);
- тепловые (пожарные);
- дымовые;
- химические (метан, углекислый газ, монооксид углерода),

а также их различные комбинации, применяемые как для расширения функциональных возможностей, так и для увеличения достоверности срабатывания датчика (сенсора, извещателя).

Рассмотрим подробнее некоторые из упомянутых типов датчиков.

1. Магнитно- контактные датчики

В общем случае представляют собой управляемый магнитным полем электрический контакт (обычно контакт герметизирован- "теркой"). Варианты исполнения – нормально-замкнутый (размыкающийся), нормально-

разомкнутый (замыкающийся), переключаемый. Механически датчик, как правило, состоит из двух частей: подвижной и неподвижной. Геркон с подключенными электропроводами обычно ставится на неподвижной части охраняемой области (оконной или дверной коробке, поверхности стола, стене и др.), а на подвижной – магнит (на створке окна, двери, настольном ценном предмете, картине и т.п.). Варианты установки – скрытая (с внедрением в материал) и открытая (на поверхности материала). Из отечественных наиболее часто встречаются извещатели типов СМК-1, СМК-3, ИО-102-4,5,6.

2. Инфракрасные датчики

По принципу действия делятся на пассивные и активные. Пассивные реагируют на тепловое излучение нагретого тела, перемещаемого в пространстве. Длина регистрируемых волн 7-10 мкм. Используются в основном для защиты помещений внутри зданий. Обнаружить их можно только визуально, а это осложняет решение задачи злоумышленника.

Формы зон обнаружения инфракрасных пассивных датчиков определяются входной оптикой, построенной в виде системы зеркал или линз Френеля (обычно изготовленных из высокоплотного полиэтилена). Зеркальные оптические системы более дороги, чем линзовые, но оптические потери у них меньше и поэтому они позволяют получить различимый сигнал на больших дистанциях. Датчики с линзами Френеля рекомендуется использовать на расстояниях не более 15 м.

При выборе инфракрасного датчика кроме специальных соображений, обусловленных решаемой задачей, следует принимать во внимание следующие конструктивные параметры датчика (чем больше их величина при прочих равных условиях – тем лучше):

- величина фокусного расстояния оптической системы (линз/зеркал) влияет на разрешающую способность оптики;
- число зон регистрации (количество сегментов оптической системы) (англ. аббревиатура – FOV (fields of view));
- размеры оптических сегментов линз/зеркал.

Недостатки инфракрасных датчиков:

- срабатывание происходит только при пересечении луча нагретым телом, а при движении тела вдоль луча реакции нет;
- при малой разнице температуры тела и среды датчик "слепнет", т.е. при температуре среды около 36 град С затруднено обнаружение человека в помещении;
- наличие в помещении в зоне обнаружения датчика автоматически включаемых источников тепла – бойлеров, обогревателей, кондиционеров, а также прямая солнечная засветка чувствительного элемента – могут приводить к ложным срабатываниям.

Активные инфракрасные датчики состоят из одной или нескольких пар "излучатель-приемник". Применяются для создания лучевых барьеров при блокировке уличных периметров охраняемой территории (датчики "внешне-

го исполнения"), отсечения периметров, коридоров, помещений, предметов внутри здания. Срабатывают при пересечении нарушителем инфракрасного луча, идущего от излучателя к приемнику. В наилучших образцах для повышения надежности реагирования предусмотрено изменение мощности излучения и чувствительности приемника при медленном изменении проницаемости среды (туман, осадки, сумеречные эффекты и т.п.), а также импульсная синхронизация излучателя и приемника. Недостатки:

- при открытой установке модулей злоумышленнику легко определить пространственную геометрию лучей и на основании этого преодолеть защищаемую зону;
- при маскированной установке расположение лучей можно определить с помощью прибора ночного видения и далее – аналогично предыдущему пункту.

Краткий словарь сокращений, наиболее часто встречающихся в англоязычных описаниях характеристик инфракрасных датчиков.

PIR – passive infrared – пассивный инфракрасный (датчик);

ABF – audio beam finder – подача звукового сигнала датчиком при пересечении луча в тестовом режиме;

AM – antimasking – антимаскирование (защита от экранирования датчика близкорасположенным непрозрачным экраном);

APS – analog pulse count – аналоговое накопление импульсов от пересечения луча;

APSP – automatic pulse signal processing – подразумевается обычно метод двухуровневой обработки сигналов от чувствительных элементов, переводящий схему датчика либо сразу в режим тревоги, либо в режим накопления импульсов от пересечения луча;

ATC – automatic temperature compensation – изменение чувствительности датчика в зависимости от температуры окружающей среды;

DOD – dual opposed detection – метод суммирования разнополярных сигналов с разных чувствительных элементов при переходе тела из одного луча в другой;

DPC – digital pulse count – цифровое (количественное) накопление сигналов с чувствительных элементов о пересечении луча;

EEA – entry/exit analyse – уровень сигнала выхода из одной зоны сравнивается с уровнем сигнала входа в другую зону;

ISG – interlock sensor geometry – конструктивное решение , в котором используются счетверенные чувствительные элементы с пересекающимися на дальних дистанциях лучами;

SPP – sequental pattern processor – для принятия решения о тревоге анализируется группа сигналов с чувствительных элементов, поступившая в течение определенного времени;

SSP – selective signal processing – селективная обработка сигнала (по времени, форме, уровню и/или их комбинациям).

3. Микроволновые (СВЧ) датчики

Работа этих датчиков основана на эффекте Доплера, который позволяет определить появление в защищаемом помещении движущегося тела любой температуры. Диапазон рабочих частот 9,5-10,5 ГГц. Излучение и прием осуществляются одной антенной. Уровень излучаемого сигнала не представляет опасности для находящихся в помещении или работающих с датчиком людей.

Диаграмма направленности датчика объемная, а в помещении за счет переотражений практически не остается "слепых" зон (если, конечно, размеры помещения меньше размеров зоны обнаружения).

Недостатки микроволновых датчиков:

- может среагировать на движение занавески из-за включившейся вентиляции
- чувствителен к движению по направлениям "к датчику – от датчика" (по оси излучения) и слабо чувствителен к движению в перпендикулярном направлении.

Оптимальным для помещений можно считать комбинированный датчик " ИК-СВЧ", одним из немногих недостатков которого будет его сравнительно с отдельными датчиками более высокая стоимость.

Вариантом микроволновых (СВЧ) датчиков являются радиолучевые сигнализаторы с разнесенными передатчиком и приемником, формирующие протяженный объемный барьер. Попадание внутрь защитного барьера постороннего предмета промодулирует излучаемый сигнал, а на это среагирует приемник. Такие датчики – прекрасное средство защиты периметров: они выдерживают перепад температур от –50 до+50 град Цельсия, дождь, ветер, туман, снег, яркое солнце и т.д.

Недостатки радиолучевых сигнализаторов:

- необходимо тщательно готовить место для их установки, так как неровности, перепады по высоте, препятствия между излучателем и приемником приводят к появлению " слепых "зон или зон нечеткого обнаружения;
- размытость границы защитного барьера может стать причиной ложного срабатывания при проезде возле нее крупногабаритного транспорта и т.п.

Поэтому по обе стороны от установленного радиолучевого сигнализатора необходимо обеспечить зону отчуждения.

4. Ультразвуковые датчики

Регистрируют изменение параметров сигнала излучения (частоты, амплитуды), отраженных от нарушителя. Конструктивно излучатель и приемник могут быть выполнены в одном корпусе (вариант малой мощности для небольших помещений) и в разных корпусах (для больших помещений и помещений сложной формы). Необходимо учитывать, что крупногабаритные неподвижные предметы создают в охраняемом помещении "слепые" зоны, а движения масс воздуха (вентиляция, кондиционер) и занавесок приводят к ложным срабатываниям.

5. Сейсмические датчики

Используются для охраны периметров зданий и территорий. Устанавливаются скрытно в грунт, ограды, стены зданий и т.п. Виды датчиков:

- жидкостный – основан на перераспределении давления в уложенных рядом шлангах с жидкостью при прохождении через них нарушителя;
- пьезоэлектрический – основан на изменении электрического сигнала при давлении на пьезоэлемент.

Наиболее известны следующие системы:

- "TESPAR" фирмы "Geoquip Ltd.";
- "PSICON";
- "GPS".

6. Электроконтактные (обрывные, натяжные и др.) датчики

Обрывные датчики обычно применяются для защиты периметров временного расположения людей, грузов, оборудования и т.п. Представляют собой одинарный либо двойной микропровод, разворачиваемый на местности. Одинарный провод замыкается в кольцо, двойной закорачивается на конце. Обрыв провода регистрируется как нарушение периметра. Развернутый провод повторно не используется.

Датчики натяжного действия состоят из нескольких рядов натянутой проволоки, подключенной к механическим выключателям или протянутой сквозь проволочные контактные кольца. При изгибе проволоки либо срабатывают выключатели, либо проволока касается кольца и сопротивление цепи меняется – система срабатывает.

Датчики в виде проволочной сетки, "путанки" из тонкой проволоки или фольги используют для защиты от проникновения в помещение через глухие поверхности (пол, потолок, крышу, стены, двери, окна). Механическое разрушение проволоки приводит к изменению сопротивления электрической цепи, что регистрируется как тревога. Датчики этого типа удобно маскировать окраской, обоями и т.п.

7. Емкостные датчики

Применяются для охраны металлических изделий (сейфов, металлических шкафов и т.д.), изолированных от пола комнаты. Принцип действия – регистрация изменения емкости между полом помещения и охраняемым объектом при приближении к объекту или касании его человеком, стоящим на полу.

Существуют емкостные системы для охраны периметров (регистрируется изменение электрической емкости чувствительного элемента при перелезании или разрушении датчика злоумышленником), например, "Радиан-13".

8. Кабельные датчики

В общем случае это распределенные периметриальные системы, в кото-

рых можно локализовать место нарушения или возгорания (в случае пожарной системы).

Главная проблема всех периметриальных систем – затруднения в различении проникновения нарушителя и изменения условий окружающей среды (погодных, фоновых электрических и магнитных помех, проезда крупногабаритного транспорта и т.п.).

Наиболее широко известны:

- охранные системы "GUARD WIRE" (Великобритания) и "ВОРОН" (Россия);
- пожарная система "PROTECTOWIRE" (США).

Во всех этих системах использованы различные по физическим принципам чувствительные элементы, но отнести их к одной группе можно по общности способа применения, который заключается в закреплении охранного кабеля по длине на ограждении (заборе, изгороди, сетке, стене и т.п.), а пожарного – вблизи пожароопасного объекта (вдоль энергокабеля в коллекторе, вокруг цистерны или танка с горючим и т.д.).

Кабель системы "GUARDWIRE" (Geoquip Ltd., UK) сконструирован так, что при его деформации даже в незначительных пределах в проводе генерируется электрический ток, который может быть зафиксирован и обработан анализатором, контролирующим форму, длительность, время и место появления сигнала. Влияние помех ослабляется как конструктивными методами (кабель помещен в полиэтиленовую оболочку, экранирован "миларом" и алюминиевой фольгой или даже оцинкованной сталью), так и программным обеспечением анализатора принимаемых сигналов. Система высококачественная, но весьма дорогая (цена 1 м кабеля около $6, а в среднем за один погонный метр периметра с учетом анализирующей аппаратуры $40).

Система "ВОРОН" построена на основе извещателя ИО-212-1"Плутон", состоящего из блоков лазерного передатчика и фотоприемника, связанных специальным световодным кабелем, оптические параметры которого меняются при его деформации. Изменение параметров световой волны регистрируется фотоприемником и анализируется процессором, заранее "обученным" на объекте имитацией проникновения. Цена системы в пересчете на 1м периметра составляет примерно $10.

Противопожарная система "PROTECTOWIRE" использует механически напряженные скрученные сталистые провода внутри одной прочной полимерной оболочки, электрически изолированные друг от друга термочувствительным полимером. Этот полимер плавится при заданной температуре окружающей среды, металлические проводники замыкаются – происходит срабатывание. Анализатор может с точностью до 0,3 м определить место срабатывания (возгорания). Фирмой "PROTECTOWIRE" разработан ряд сигнальных кабелей для различных температур и сред различной агрессивности. В настоящее время разработан и находится в стадии сертификации "кабель с предупреждением" – кабель, содержащий два полимера с разными температурами плавления и три электрических проводника. Первый полимер плавит-

ся при повышении температуры среды выше нормы, но ниже температуры возгорания – на анализатор поступает сигнал "предупреждение".

Цена за 1 м кабеля "PROTECTOWIRE" составляет в среднем $5.

9. Видеосигнальные датчики

Распространенное название "MOVE-DETECTOR", т.е. детектор движения. Принцип действия: регистрация изменения видеосигнала в заданных оператором областях изображения. Обычно дополняют охранные видеокамеры и бывают цифровыми и аналоговыми. Соответственно, цифровые многофункциональнее и дороже, а аналоговые проще и дешевле. Конструктивно обычно снабжены локальным акустическим сигнализатором ("пищалкой") и "ALARM" – выходом управления внешними устройствами (охранной сигнализацией, видеомультиплексором или видеомагнитофоном).

10. Микрофонные датчики

Наиболее распространены построенные на микрофонном принципе детекторы разбивания стекла (glass-break detectors).

Принцип действия: постоянно анализируется акустическая обстановка в помещении и при совпадении поступившего сигнала с сигналом, хранящимся в базе данных датчик срабатывает. Сложные алгоритмы спектрального анализа сигналов, частотного разделения и т.п. используются для уменьшения количества ложных срабатываний.

Дистанция обнаружения детектора разбивания стекла зависит от следующих факторов:

- типа и размера защищаемого стекла;
- размера и формы помещения;
- материалов, покрывающих стены и пол;
- расстановки мебели в помещении;
- наличия и вида занавесей, ширм и т.п.;
- фонового акустического шума;
- угла установки датчика по отношению к стеклу.

Недостатки датчика определены тем, что в базу данных нельзя внести все возможные на свете типы стекол – т.е. остаются белые пятна. Но опыт показывает, что все-таки 95% перекрыты, а несомненное удобство и изящество установки в совокупности делают эти детекторы привлекательными.

11. Фотоэлектрические датчики

Работа этих датчиков основана на прерывании нарушителем луча света произвольного диапазона, падающего на приемник.

Требования к установке фотоэлектрических датчиков:

- приемник и передатчик должны располагаться на капитальных недеформируемых конструкциях (для сохранения их взаиморасположения);

- должно быть исключено попадание на приемник прямых и отраженных солнечных лучей, света автомобильных фар и других мощных световых источников;
- между излучателем и приемником должен быть коридор сечением 0,5Х 0,5 м, свободный от затеняющих или движущихся предметов (занавесей и т.п.).

Некоторые датчики выполнены по однопозиционной схеме, т.е. в одном блоке совмещены излучатель и приемник, а поток формируется с помощью пассивных отражателей (извещатель охранно-пожарный линейный фотоэлектрический "Вектор-3").

12. Поршневые ("subsonic"-эффект)

Реагируют на движение масс воздуха в помещении, инициированное открыванием наружного распашного окна или двери (на открывание сдвижных окон и дверей, а также внутренних распашных окон и дверей – не реагируют).

На наш взгляд, такие датчики имеет смысл использовать либо в специальных помещениях (глухая кладовая с одной дверью и т.п.), либо реагируя на срабатывание системы собственными силами, так как должен быть выставлен очень шаткий баланс чувствительности датчика к проникновению и отсутствия ложных срабатываний в условиях, отличающихся от "боевых".

13. Основные сведения о пожарных извещателях

Пожарные извещатели принято делить на следующие типы:

- дымовые – обнаруживающие аэрозольные продукты термического разложения;
- газовые – обнаруживающие невидимые газообразные продукты термического разложения;
- тепловые – реагирующие на конвективное тепло от очага пожара;
- пламени – реагирующие на оптическое излучение пламени очага пожара.

Если применение автоматических пожарных извещателей невозможно или нецелесообразно, то используют ручные пожарные извещатели или кнопочные сигнализаторы.

Каналы связи обычно бывают реализованы в виде:

- специально проложенных проводных или оптоволоконных линий;
- эфирной радиосвязи;
- инфракрасной связи;
- оптической (в том числе лазерной) связи;
- имеющихся на объекте линий:
  а) телефонных;
  б) электрических силовых;
  в) локальной компьютерной сети.

3.2. Источники электропитания

Большинство систем ОПС требуют переключения на резервный источник питания в случае снижения сетевого напряжения ниже допустимого уровня или отключения сети. При восстановлении нормального уровня сетевого напряжения система переключается на питание от первичной сети. Такой режим работы ОПС обеспечивают источники резервного питания, которые имеют в своем составе аккумулятор.

При установке источников резервного питания ОПС в реконструируемых зданиях возникают проблемы, связанные со сложностью, а иногда и невозможностью прокладки линий первичного электропитания первой категории до оптимальных мест размещения источников. В таких случаях задачу можно решить питанием источника от низковольтной сети, размещая электропроводку в низковольтных кабельных стволах.

Кроме того, источник должен обладать свойствами, типичными для вторичных источников электропитания:

- защитой источника электропитания от перегрузки по току и короткого замыкания в цепях подключения нагрузки;
- защитой датчиков ОПС в случае отказа источника и появления на выходе напряжения, превышающего номинальное;
- защитой источника по первичной цепи.

Наличие в источнике аккумулятора требует контроля за его состоянием. Поэтому источник резервного электропитания должен также осуществлять:

- контроль уровня заряда аккумулятора и индикацию состояния "Аккумулятор разряжен";
- автоматический заряд аккумулятора;
- защиту аккумулятора от глубокого разряда.

При размещении источников по территории больших объектов требуется обеспечить индикацию аварийных состояний (отсутствие напряжения сети переменного тока, разряженный аккумулятор) на пульте централизованного наблюдения (ПЦН).

Источники обычно имеют моноблочную конструкцию и выполнены по модульному принципу. В состав источника входят модули выпрямителя, стабилизатора, устройства контроля и аккумулятор.

Для работы от низковольтных линий питания иногда реализуется специальный заказной вариант конструктивного исполнения источника резервного электропитания в виде двух блоков. В первом блоке размещается понижающий трансформатор, на выходе которого формируется напряжение для низковольтных линий питания. Напряжение с выхода первого блока по низковольтным линиям питания передается на второй блок, в котором размещается выпрямитель, стабилизатор, устройство контроля и стабилизатор. Второй блок размещается вблизи подключаемых к нему устройств ОПС.

Такое подключение позволяет уменьшить сечение проводов линий питания по сравнению с системой, когда все составные части источника резервного электропитания находятся в одном блоке на большом расстоянии от

устройств ОПС. Возможен вариант построения системы, когда к одному блоку с мощным трансформатором подключается несколько блоков второго типа, распределенных по территории объекта. Этот подход способствует снижению стоимости системы электропитания.

Для стабилизации выходного напряжения применяются обычно схемы импульсных стабилизаторов, использующих принцип широтно-импульсной модуляции, что обеспечивает высокий коэффициент полезного действия и позволяет снизить температуру силовых элементов схемы.

Устройством контроля вырабатывается сигнал "Авария сети питания", если напряжение сети переменного тока ниже нормы или отсутствует.

В этом случае питание устройств ОПС осуществляется от аккумулятора, и на панели источника включается соответствующая индикация. Если нормальное состояние сети переменного тока восстанавливается, то сигнал "Авария сети питания" снимается и возобновляется работа импульсного стабилизатора.

С помощью устройства контроля периодически (обычно один раз примерно в 20 минут) производится проверка напряжения на выходе аккумулятора при реальной нагрузке. Если оно меньше допустимого уровня, то формируется сигнал "Аккумулятор разряжен" и включается соответствующая индикация на панели источника электропитания. Режим проверки может быть выключен, например, в случае отсутствия аккумулятора в составе источника.

Сигналы "Авария сети питания", "Аккумулятор разряжен" могут быть переданы на пульт централизованного наблюдения.

Если выходной ток нагрузки источника начинает превышать номинальную величину, то включается электронная схема защиты. После снятия перегрузки источник продолжает нормально функционировать.

Для защиты устройств ОПС, подключенных к источнику, от повышенного напряжения по цепям питания, которое может появиться при выходе из строя элементов импульсного стабилизатора, используется тиристорная схема, отключающая нагрузку от выхода источника электропитания.

Подключение аккумулятора резервного источника для заряда осуществляется двумя способами. Первый из них предназначен для герметичных кислотно-свинцовых аккумуляторов, которые могут работать в буферном режиме.

Второй способ основан на использовании схемы ограничения тока заряда, что позволяет применять аккумуляторы не только кислотно-свинцового, но и других типов, а также заряжать аккумуляторы с глубокой степенью разряда.

В обоих случаях аккумулятор подключается к нагрузке через устройство, ограничивающее его разряд. В случае разряда аккумулятора до предельно допустимого напряжения срабатывает схема ограничения разряда, отключающая его от устройств ОПС.

3.3. Приемно- контрольный прибор (ПКП)

Приемно-контрольный прибор – центральное звено, "мозг " системы ОПС- выбирается в соответствии с задачами, решаемыми системой. Он обычно позволяет:

- контролировать состояние компонентов ОПС (структурные единицы определяются топологией системы) на уровне "включено-выключено", "неисправность", "тревога", "попытка вскрытия датчика (или центрального блока) – саботаж";
- записывать и хранить указанные выше сигналы;
- включать различные исполнительные устройства;
- информировать о событиях пульт центрального наблюдения.

Общая классификация технических средств ОПС приводится в справочном приложении 2 к ГОСТ 26342-84* "Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры."

Приемно- контрольные приборы подразделяют:

1) *по информационной емкости:*
   - малой информационной емкости – до 5 шлейфов сигнализации;
   - средней информационной емкости – от 6 до 50 шлейфов сигнализации;
   - большой информационной емкости – свыше 50 шлейфов сигнализации.
2) *по информативности:*
   - малой информативности – до 2 видов извещений;
   - средней информативности – от 3 до 5 видов извещений;
   - большой информативности – свыше 5 видов извещений.
3) *по возможности резервирования составных частей:*
   - без резервирования;
   - с резервированием.
4) *по назначению:*
   - для охраны квартир граждан;
   - для охраны объектов народного хозяйства.

Наиболее известные иностранные фирмы-производители ПКП "Ademco" (USA), "PARADOX" (UK), "DSC" (Canada), "CROW", "ROKONET", "VISONIC" (Israel), CERBERUS (Helvetia) и др.

3.4. Монтаж технических средств сигнализации

3.4.1. Монтаж охранных, охранно-пожарных и пожарных извещателей

Выбор типов охранных и охранно-пожарных извещателей, их количества, места установки и методы монтажа должны определяться в соответствии с требованиями действующих нормативных документов, с учетом физико-химических свойств веществ и материалов, используемых в защищаемом помещении (объекте), видом и значимостью охраняемого объекта, принятой

тактикой охраны, объектовой помеховой обстановкой, размерами и конструкцией защищаемых элементов, техническими характеристиками извещателей. При этом должно быть исключено образование непросматриваемых ("мертвых", "слепых") зон.

Размещение и монтаж охранно-пожарных извещателей должны производиться в соответствии с проектом (актом обследования), требованиями СНиП, технологическими картами и инструкциями.

В защищаемой зоне, а также вблизи нее на расстояниях, указанных в технической документации, не должно быть посторонних предметов, изменяющих зону чувствительности извещателей. При установке в одном помещении нескольких оптико-электронных или радиоволновых извещателей необходимо применять извещатели с разными частотными литерами.

Монтаж емкостных, оптико-электронных, радиоволновых, ультразвуковых и комбинированных извещателей должен производиться на жестких, устойчивых к вибрации опорах (капитальных стенах, колоннах, столбах и т.п.) с помощью котировочных узлов, кронштейнов или подставок и исключать возможность ложного срабатывания извещателей по этой причине.

3.4.2. Монтаж приемно-контрольных приборов, сигнально-пусковых устройств и оповещателей

Размещение приемно- контрольных приборов (ПКП) должно быть проведено в соответствии с требованиями СНиП 2.04.09.

Установка ПКП малой информационной емкости должна производиться:

- при наличии специально выделенного помещения – на высоте, удобной для обслуживания
- при отсутствии специально выделенного помещения – на высоте не менее 2,2 м.

Установка ПКП в общедоступных местах должна производиться в запираемых металлических шкафах, конструкция которых не влияет на работоспособность приборов. Вне помещения ПКП устанавливаются в металлических шкафах или ящиках, блокируемых на открывание.

Установка ПКП средней и большой информационной емкости должна производиться в выделенных помещениях: на столе, стене или специальной конструкции, на высоте, удобной для обслуживания, но не менее 1 м от уровня пола. Не допускается установка ПКП:

- в сгораемых шкафах;
- на расстоянии менее 1 м от отопительных систем;
- во взрывоопасных помещениях;
- в помещениях пыльных и особо сырых, а также содержащих пары кислот и агрессивных газов.

Световые и звуковые оповещатели должны устанавливаться в удобных для визуального и звукового контроля местах.

При наличии на объекте нескольких ПКП световой оповещатель подключается к каждому прибору, а звуковой оповещатель допускается делать общим.

Требования пожарной безопасности при монтаже технических средств (ТС) сигнализации в пожароопасных зонах следующие.

ТС сигнализации, работающие от сети переменного тока, как правило, должны устанавливаться вне пожароопасных зон. Установка средств в пожароопасных зонах должна соответствовать требованиям правил устройства электроустановок (ПУЭ).

При монтаже ПКП и СПУ, охранных и охранно-пожарных извещателей или их отдельных блоков на горючих основаниях (деревянная стена, монтажный щит из дерева или ДСП толщиной не менее 10 мм), необходимо применять огнезащитный листовой материал (металл толщиной не менее 1 мм, асбоцемент, гетинакс, текстолит, стеклопластик толщиной не менее 10 мм) закрывающий монтажную поверхность под прибором, или специальный металлический щиток по ГОСТ 8709.9413. При этом листовой материал должен выступать за контуры установленного на нем прибора не менее чем на 100 мм.

При монтаже нескольких ПКП в ряд должны соблюдаться следующие расстояния:

- между ПКП в ряду – не менее 50 мм;
- между рядами ПКП – не менее 200 мм.

Расстояние от открыто смонтированных извещателей, работающих от сети переменного тока, до расположенных в непосредственной близости горючих материалов или веществ должно быть не менее 600 мм.

При установке световых и звуковых оповещателей, работающих от сети переменного тока, внутри помещения расстояние от колбы лампы до деревянных стен, потолка, оконных рам должно быть не менее 50 мм. Не допускается применение ламп накаливания мощностью более 25 Вт.

3.4.3. Монтаж электропроводок технических средств сигнализации

Монтаж электропроводок технических средств сигнализации должен выполняться в соответствии с проектом (актом обследования), типовыми проектными решениями и с учетом требований СНиП 2.04.09, 3.05.06, ПУЭ, "Общей инструкции по строительству линейных сооружений городских телефонных сетей", "Инструкции по монтажу сооружений и устройств связи, радиовещания и телевидения".

Прокладка незащищенных проводов и кабелей через помещения, которые не подлежат защите, должна производиться скрытым способом или в металлических тонкостенных трубах. При прокладке скрытым способом провода и кабели сигнализации должны быть проложены в отдельной штробе.

Прокладка проводов и кабелей по стенам внутри охраняемых помещений должна производиться на расстоянии не менее 0,1 м от потолка и, как правило, на высоте не менее 2,2 м от пола. При прокладке проводов и кабе-

лей на высоте менее 2,2 м от пола должна быть предусмотрена их защита от механических повреждений.

Соединения и ответвления проводов и кабелей должны производиться в соединительных или распределительных коробках способом пайки или с помощью винтов.

3.5. Пусконаладочные работы при установке ТС сигнализации

Пусконаладочные работы должны выполняться монтажно-наладочной организацией в соответствии с требованиями СНиП 3.05.06-85. Для проведения пусконаладочных работ заказчик должен:

- согласовать с монтажно-наладочной организацией сроки выполнения работ, предусмотренные в общем графике;
- обеспечить наличие источников электроснабжения;
- обеспечить общие условия безопасности труда.

До начала пусконаладочных работ в процессе производства монтажных работ должны быть проведены индивидуальные испытания (настройка, регулировка, юстировка) ПКП, СПУ, извещателей и т.п. в соответствии с техническими описаниями, инструкциями, ПУЭ.

Производство пусконаладочных работ производится в три этапа:

1) подготовительные работы;
2) наладочные работы;
3) комплексная наладка технических средств.

На этапе подготовительных работ должны быть:

- изучены эксплуатационные документы на ТС сигнализации;
- оборудованы необходимым инвентарем и вспомогательной оснасткой рабочие места наладчиков.

На этапах наладочных работ и комплексной наладки должна проводиться корректировка ранее проведенной регулировки ТС, в том числе: доведение параметров настройки до значений, при которых ТС могут быть использованы в эксплуатации, вывод аппаратуры на рабочий режим, проверка взаимодействия всех ее элементов в режимах "Тревога", "Неисправность", "Пожар" и т.п.

Пусконаладочные работы считаются законченными после получения предусмотренных проектом и технической документацией параметров и режимов, обеспечивающих устойчивую и стабильную работу ТС (без ложных сигналов тревоги).

3.5.1. Маркировка и пломбирование ТС сигнализации

ПКП и СПУ по окончании монтажно-наладочных работ должны быть промаркированы с указанием:

- для объектовых ТС сигнализации – наименования защищаемых помещений и назначения прибора;

- для периметриальных ТС сигнализации – схемы периметра объекта с защищаемыми зонами.

После приемки ТС сигнализации в эксплуатацию монтажно-наладочная организация должна опломбировать те части прибора, к которым имел доступ ее представитель в процессе монтажа и наладки, проверить наличие и целостность пломб предприятий-изготовителей на приборах.

3.5.2. Приемка в эксплуатацию ТС сигнализации

Приемка в эксплуатацию ТС сигнализации должна производиться в соответствии с требованиями СНиП 3.01.04-87.

Для приемки в эксплуатацию ТС сигнализации приказом руководства организации (предприятия) заказчика назначается рабочая комиссия.

В состав рабочей комиссии включаются представители:

- организации (предприятия) заказчика (председатель комиссии);
- монтажно-наладочной организации;
- подразделения охраны;
- органов государственного пожарного надзора.

Комиссия должна приступить к работе по приемке ТС сигнализации не позднее трех суток (не считая выходных и праздничных дней) со дня уведомления монтажно-наладочной организации о готовности ТС к сдаче.

При приемке в эксплуатацию ТС сигнализации монтажно-наладочная организация должна предъявить рабочей комиссии:

- исполнительскую документацию (комплект рабочих чертежей с внесенными в них изменениями или акт обследования);
- техническую документацию предприятий-изготовителей;
- сертификаты, технические паспорта или другие документы, удостоверяющие качество материалов, изделий и оборудования, применяемых при производстве монтажных работ;
- производственную документацию (обязательное приложение).

Приемка в эксплуатацию ТС сигнализации без проведения комплексной наладки и апробирования не допускается.

При приемке в эксплуатацию выполненных работ по монтажу и наладке ТС сигнализации рабочая комиссия производит:

- проверку качества и соответствия выполненных монтажно-наладочных работ проектной документации предприятий-изготовителей;
- измерение сопротивления изоляции шлейфа сигнализации (должно быть не менее 1 МОм);
- измерение сопротивления шлейфа сигнализации;
- испытания работоспособности смонтированных ПКП, СПУ.

В необходимых случаях комиссия проводит и другие проверки и измерения параметров, оговоренных техническими условиями на смонтированную аппаратуру. Методика испытаний определяется в каждом конкретном случае рабочей комиссией.

При обнаружении отдельных несоответствий выполненных работ проектной документации или акту обследования, а также требованиям настоящих правил, комиссия должна составить акт о выявленных отклонениях, на основании которого монтажно-наладочная организация устраняет их в десятидневный срок и вновь предъявляет ТС сигнализации к сдаче.

ТС сигнализации считаются принятыми в эксплуатацию, если проверкой установлено:

- все элементы строительных конструкций и зоны по периметру объекта заблокированы согласно проекту или акту обследования;
- монтажно-наладочные работы выполнены в соответствии с требованиями настоящих правил, технологическими картами и технической документацией предприятий-изготовителей;
- результаты измерений в пределах нормы;
- испытания работоспособности ТС сигнализации дали положительный результат, причем средства пожарной сигнализации должны обеспечивать в случаях, предусмотренных проектом, отключение систем вентиляции, включение систем дымоудаления и подпора воздуха в лестничные клетки и тамбурные шлюзы при пожаре.

Прием ТС сигнализации в эксплуатацию должен оформляться актом установленной формы согласно обязательному приложению *2* РД.

Необходимость подключения объектовой сигнализации к пультам централизованного наблюдения определяется подразделениями охраны с участием представителей заказчика и органов пожарной охраны.

3.5.3. Гарантия

Монтажно-наладочная организация гарантирует безотказную работу смонтированных ТС сигнализаций в течение 12 месяцев со дня приемки в эксплуатацию и обязана в сроки, указанные в акте о выявленных дефектах, устранить несправности, возникшие по ее вине.

Акт составляется комиссией с участием представителей заказчика, монтажно-наладочной организации, подразделения охраны, пожарной охраны, организации, осуществляющей эксплуатацию ТС сигнализации.

Для участия в работе комиссии, организации обязаны командировать своих представителей в пятидневный срок со дня получения письменного уведомления заказчика. При неявке в установленный срок представителя любой организации из вышеперечисленных, акт о выявленных дефектах составляется без его участия.

Монтажно-наладочная организация не несет ответственность:

- за неисправности, возникшие из-за несоблюдения правил эксплуатации;
- за дефекты, возникшие в ТС сигнализации (переданных в монтаж заказчиком, подразделением охраны) в процессе эксплуатации по вине предприятий-изготовителей.

3.6. Организация содержания, технического обслуживания и ремонта охранно-пожарной сигнализации

3.6.1. Техническое обслуживание (ТО) средств сигнализации

Основными задачами ТО являются:

- обеспечение устойчивого функционирования ТС сигнализации;
- контроль технического состояния ТС;
- выявление и устранение неисправностей и причин ложных тревог, уменьшение их количества;
- ликвидация последствий воздействия на ТС климатических, технологических и других неблагоприятных условий;
- анализ и обобщение сведений по результатам выполнения работ, разработки мероприятий по совершенствованию форм и методов ТО.

ТО может быть плановым (регламентным) и неплановым (по техническому состоянию).

Плановое ТО включает в себя проверку:

- шлейфов сигнализации;
- ПКП и СПУ;
- сложных извещателей;
- устройств электропитания;
- общей работоспособности системы (комплекса).

Результаты проведения планового ТО регистрируют в специальном журнале.

Неплановое ТО проводят при:

- поступлении ложных сигналов тревоги с охраняемого объекта;
- отказа аппаратуры;
- ликвидации последствий неблагоприятных климатических условий, технологических и других воздействий;
- заявке пользователя (собственника охраняемого объекта).

3.6.2. Ремонт ТС сигнализации

Ремонты бывают:

- текущие и капитальные – для шлейфов сигнализации (ШС);
- средние и текущие – для аппаратуры.

Текущий ремонт ШС – замена отдельных вышедших из строя компонентов (извещателей, установочных элементов, участков соединительных линий).

Капитальный ремонт ШС – демонтаж и полная замена извещателей, соединительных линий, установочных элементов. Проводится при невозможности дальнейшей эксплуатации ШС или при капитальном ремонте охраняемого объекта.

Средний ремонт аппаратуры – частичная или полная ее разборка, восстановление или замена составных частей.

Текущий ремонт аппаратуры – замена отказавших легкосъемных элементов.

3.7. Взаимодействие служб, обеспечивающих охрану объекта

Пользователи системы сигнализации (собственники охраняемого объекта) должны иметь постоянную связь с организациями и службами, обеспечивающими охрану объекта и безотказное функционирование ТС.

Время прибытия на охраняемый объект специалистов по восстановлению работоспособности системы при ее отказе не должно превышать 4 ч (за исключением труднодоступных объектов). В случае невозможности в срок выполнить восстановительные работы ремонтная служба должна информировать об этом пользователя системы.

Порядок взаимодействия пользователя (хозоргана, собственника) со службами, обеспечивающими охрану объекта, выполнение нормативов по организации и несению охраны, регламентируют действующими законодательными и нормативными актами, ведомственными актами и служебными инструкциями.

3.7.1. Регистрация сигналов тревоги и отключения системы

Регистрация сигналов тревоги, выдаваемых системой, должна вестись в форме записей, содержащих дату и время приема сигнала тревоги, вида сигнала, места его возникновения; хронометраж проведения мероприятий по реагированию на сигналы.

Регистрация случаев отключения системы в целом или ее отдельных фрагментов должна вестись в форме записей, содержащих дату и время отключения и причину этого, дату и время повторного включения. Пользователь (собственник охраняемого объекта) или его представитель должен подтвердить каждый случай отключения системы и его последствия .

3.7.2. Действия персонала в случае сигнала тревоги

Действия персонала объекта по сигналам тревоги системы должны быть регламентированы специальными инструкциями, согласованными со службами обеспечения охраны объекта. Инструкции должны включать в себя сведения о том, как персонал должен реагировать, какие предпринимать действия, какие использовать средства связи и т.п.

Служебные инструкции, регламентирующие действия персонала объекта по сигналам тревоги должны учитывать:

- тип, значимость и режим работы объекта;
- характер, значимость и места расположения охраняемых ценностей;
- принятые вид и тактику охраны;
- наличие на объекте людей во время действия системы;

- дислокацию объекта на местности;
- средства связи, имеющиеся на объекте.

3.8. Принципы выбора пожарных извещателей для защиты объекта

Для обеспечения надежной работы систем пожарной сигнализации следует правильно выбрать типы и расположение пожарных извещателей: они должны обеспечивать своевременность обнаружения пожара и не давать ложных срабатываний при длительной эксплуатации.

Время обнаружения пожара зависит от эффективности пожарного извещателя, а время передачи сообщения – от технических характеристик системы связи.

Для оценки времени обнаружения пожара расчетом или экспериментально определяют динамику развития пожара – концентрацию дыма, величину температуры, наличие излучения в различных точках помещения. По техническим характеристикам извещателей подбирается такой, время срабатывания которого будет меньше допустимого времени обнаружения пожара.

Далее следует сопоставить условия эксплуатации выбранного извещателя на данном объекте с возможностями его конструкции. Если хотя бы один из параметров извещателя не соответствует условиям эксплуатации, то этот извещатель не подходит для данного объекта.

При анализе размещения извещателя на объекте главное – правильно определить защищаемую им площадь. Для этого надо учесть высоту и форму помещения, наличие различных помех. Защищаемая площадь не должна превышать указанную в паспорте, но для увеличения скорости и достоверности срабатывания извещателя эта площадь может быть уменьшена.

3.8.1. Требования СНиП к размещению пожарных извещателей

Общие требования

Количество автоматических пожарных извещателей (АПИ) определяется необходимостью обнаружения загораний по всей контролируемой площади помещений (зон), а для световых извещателей – и оборудования.

Если установка пожарной сигнализации предназначена для управления автоматическими установками пожаротушения, дымоудаления и оповещения о пожаре, каждую точку защищаемой поверхности необходимо контролировать не менее, чем двумя АПИ.

Дымовые и тепловые пожарные извещатели следует устанавливать, как правило, на потолке. При невозможности установки АПИ на потолке допускается установка их на стенах, балках, колоннах, подвеска на тросах. В этих случаях извещатели необходимо размещать на расстоянии не более 300 мм от потолка, включая габариты извещателя.

4. ВИДЕОНАБЛЮДЕНИЕ

4.1. Чего хочет потребитель?

Первое, и самое важное, без чего нельзя начинать проектирование охранной видеосистемы — знание и понимание запросов потребителя. Потребители могут быть технически грамотными и многие из них могут хорошо разбираться в системах охранного телевидения. Но чаще всего они не знакомы с последними техническими достижениями и возможностями каждого компонента.

Прежде всего следует уяснить общую концепцию контроля и видеонаблюдения, которые требуются потребителю: будет ли вестись постоянный мониторинг видеокамерами и 24-х часовая работа персонала безопасности, или планируется работа в автоматическом режиме (обычно с постоянной записью), или же предполагается сочетание обоих вариантов наблюдения. Как только вы поймете, чего хочет заказчик, было бы неплохо разъяснить ему, чего можно добиться с помощью предлагаемого оборудования. Работать с небольшими и простыми системами достаточно легко, но как только они увеличиваются до 10 видеокамер и более (некоторые из которых могут быть установлены на поворотных устройствах), нескольких видеомониторов, более одного места видеонаблюдения, нескольких датчиков тревоги и видеомагнитофонов — задача намного усложнится.

Существует также множество неизвестных переменных, которые необходимо учитывать при разработке системы охранного телевидения. Что случится, если одновременно сработают несколько датчиков тревоги? Какой видеомонитор должен показывать «тревожные» видеокамеры? Будет ли записываться изображение по сигналу тревоги, если видеомагнитофон(-ы) в это время воспроизводит(-ят) запись? Какой уровень приоритета для каждого оператора? И так далее.

Эти переменные определяют сложность системы и, как в математике, чтобы решить задачу с большим количеством переменных, необходимо знать большее количество параметров. Потребитель может указать специализированные параметры, но только после того, как он поймет технические возможности оборудования.

Понятно, что для эксперта охранного телевидения, императивом является знание компонентов, аппаратного оборудования и программного обеспечения, которое он предлагает, и пути наилучшего из возможных решения требуемой задачи.

Не следует утверждать, что система будет делать то-то и то-то, если эксперт не уверен и не может гарантировать, что она выполнит все обещанное вами.

Поэтому для разработки хорошей, функциональной системы необходимо знать используемые компоненты, их преимущества и ограничения, как они взаимосвязаны и как потребитель хочет их использовать.

Первые требования, несомненно, будут соблюдены, поскольку эксперт не может заниматься проектированием охранного телевидения, если не владеет базовыми знаниями о таких системах. Последнее – то есть желания потребителя – можно определить в ходе телефонного разговора или при встрече с ним.

Следующее, что необходимо сделать – это провести обследование объекта в месте размещения видеосистемы. Ниже приведены вопросы, которые необходимо задать потребителю до начала разработки системы и до или во время обследования места установки.

- Какова основная задача проектируемой видеосистемы?

Если это сдерживающая злоумышленников система, то необходимо так спланировать размещение видеокамер и видеомониторов, чтобы они были видны публике. Если система предназначается для скрытого видеонаблюдения, то необходимо уделить особое внимание типу и размеру видеокамеры, ее маскировке, скрытности проводки и аналогичным проблемам, а также выяснению предполагаемых сроков ее установки (возможно, через несколько часов).

- Кто будет оператором (-ами)?

Если планируется 24-х часовая работа охраны, реакция системы на сигнал тревоги должна быть другой, чем в автоматическом режиме или при работе в частично автоматическом режиме.

- Это будет черно-белая или цветная видеосистема?

От этого будет зависеть стоимость системы и ее чувствительность. Следовательно, необходимо изучить освещенность в зоне установки системы. Цветное изображение даст большую информацию о деталях наблюдаемых объектов, но если предполагается наблюдение при очень низком уровне освещенности или при инфракрасном освещении, то не имеется других вариантов, кроме использования черно-белых видеокамер (если только заказчик не согласен оплатить некоторые новые, имеющиеся на рынке видеокамеры, которые переключаются с цветного на черно-белый режим). Стоимость цветной системы диктуется не только видеокамерами, но и видеомониторами, видеомультиплексорами и/или видеоквадраторами (разделителями экрана), если таковые требуются.

- Сколько видеокамер будет использоваться?

Для небольшой системы с числом видеокамер до 6 достаточно одного видеокоммутатора или видеомультиплексора, для более крупной системы скорее всего понадобится матричный видеокоммутатор или большее число коммутаторов или видеомультиплексоров.

- Сколько видеокамер будет с фиксированной установкой и объективом с постоянным фокусным расстоянием и сколько установлено на поворотных устройствах и имеет вариообъектив?

Между этими видами видеокамер существует большая ценовая разница. Если вместо видеокамеры с фиксированным фокусным расстоянием используется PTZ-камера, дополнительную стоимость составят варио-

объективы (в противоположность объективам с фиксированным фокусным расстоянием), поворотное устройство или скоростная поворотная видеокамера, приемник сигналов телеуправления и пульт управления. Но преимущества, получаемые потребителем от системы с PTZ-камерой, увеличиваются в четыре раза. Если вдобавок к этому PTZ-камеры имеют предустановку, то гибкость и эффективность системы возрастает еще в несколько раз по сравнению с системой, использующей фиксированную видеокамеру. Если в систему входит только одна PTZ-камера и 6 фиксированных, то может потребоваться матричный видеокоммутатор, и стоимость всей системы значительно возрастет (по сравнению с системой, состоящей только из фиксированных видеокамер). В качестве альтернативы, управлять одной PTZ-камерой можно и при помощи специального цифрового контроллера или контроллера непосредственного управления электродвигателями поворотного устройства, но это также значительно увеличит стоимость системы. Поэтому, если задача требует применения PTZ-камеры, то экономичнее иметь несколько таких камер.

- Сколько потребуется видеомониторов и пультов управления?

Для небольшой системы логично предложить один видеомонитор и один пульт управления, но как только увеличивается количество операторов и/или одновременно просматриваемых каналов и управляемых видеокамер, спланировать практичную и эффективную систему становится труднее. В этом случае – для планирования расположения оборудования и соединений – необходимо обследование диспетчерской (помещения охраны).

- Будет ли система использоваться для мониторинга в реальном режиме времени (что требует немедленной реакции на тревоги), или будет осуществляться запись видеосигналов для последующего просмотра и проверки?

Ответ на этот вопрос определяет, понадобятся ли вам видеомагнитофон(-ы) с видеомультиплексором(-ами). Если у вас есть матричный видеокоммутатор, вам в любом случае потребуется еще и видеомультиплексор, а может даже два. Помните, что планируемые режимы «time lapse» зависят от того, как часто можно будет менять видеокассеты, а это определяет время обновления информации с каждой записываемой видеокамеры. Если вы хотите минимизировать время задержки при видеозаписи, то лучше выбрать два 9-ти (или 8-ми) канальных видеомультиплексора вместо одного 16-ти канального.

- Какие средства передачи видеосигналов могут быть использованы на охраняемой территории?

Обычно, по неписаным правилам используется коаксиальный кабель и в соответствии с этим должна планироваться установка системы. Однако иногда нет иного выбора, и приходится использовать только передачу по радиоканалу или даже волоконно-оптический кабель, что намного увеличивает общую стоимость системы. Если охраняемая территория подвержена регулярной грозовой активности, вам лучше с самого начала предложить волоконно-оптический кабель и объяснить клиенту долгосрочную экономию это-

го варианта. Необходимо выяснить как можно больше об окружающей среде, в которой будет функционировать система, что в ней физически возможно, а что невозможно, и только после этого планировать приемлемые средства передачи видеосигналов и данных.

- Последнее и, пожалуй, самое важное, что необходимо выяснить, это объем средств, планируемых на систему.

Это определит и уточнит некоторые предыдущие вопросы и может заставить вас либо изменить тип оборудования и уменьшить количество видеокамер, либо сузить предполагаемый режим работы системы. Это один из самых важных факторов, но он не должен приводить к снижению качества проектируемой системы до такого уровня, что система не сможет удовлетворительно функционировать.

Если размер бюджета недостаточен для желаемой системы, то можно предложить заказчику два варианта: систему, которая будет работать в соответствии с его требованиями (даже если ее стоимость и превышает бюджет), и еще одну, вписывающуюся в рамки запланированных средств и содержащую столько функций, сколько позволяет бюджет. Скорее всего, это вынудит уменьшить число видеокамер или отказаться от PTZ-камер в пользу фиксированных видеокамер.

Наиболее весомый аргумент, который должен выдвинуть эксперт, предлагая свою разработку, состоит в том, что охранная видеосистема должна быть, прежде всего, системой безопасности, что возможно только в том случае, если она будет соответственно разработана. Хорошо спроектированная система – это экономия средств в долгосрочной перспективе.

4.2. Концепции систем видеонаблюдения

Система видеонаблюдения предназначена в первую очередь для применения в тех случаях, когда необходимо иметь однозначное представление о происходящем событии, но нет возможности обеспечив наблюдение глазами охранника.

Поскольку трудно рассчитывать на то, что оператор у пульта наблюдения и контроля со 100% гарантией своевременно заметит изменение в контролируемой области просто наблюдая за мониторами, система видеонаблюдения должна быть сопряжена с некоторым дополнительными устройствами обнаружения перемещений, подающими звуковой сигнал для привлечения внимания дежурного оператора.

Наибольшая неопределенность при анализе обстановки на внешнем периметре объекта связана с большой вероятностью ложного срабатывания. Сочетание системы обнаружения движения с системой видеонаблюдения, возможно, является оптимальным разрешением этой неопределенности при условии реализации в системе надлежащего выбора камеры и места ее установки.

При подборе и установке видеокамеры необходимо принимать во внимание следующие параметры:

- высота над поверхностью земли;
- угол обзора;
- расстояние до наблюдаемой области;
- направление обзора, фиксированная или переменная линия обзора;
- наличие естественного или искусственного освещения, уровни освещения;
- положение солнца в разное время года;
- положение относительно соседних камер;
- "мертвые" и перекрывающиеся зоны;
- способы защиты от природных явлений, хищений и умышленного вывода из строя;
- требуемая длина соединительного кабеля;
- простота обслуживания;
- стоимость.

Изображение человека на контрольном мониторе при максимальном расстоянии в рабочем диапазоне камеры должно быть не менее 25 мм.

Учет указанных параметров облегчает задачу подбора видеокамеры для конкретной точки.

Для уменьшения неопределенности необходимо подобрать камеру, обеспечивающую хорошее качество изображения. При этом имеют значение освещение, кабель и монитор, но качество камеры предопределяет общее качество работы системы.

Ограничивающим фактором является элемент, принимающий изображение внутри камеры (мишень), аналогичный сетчатке глаза. Электронная начинка камеры также не должна создавать проблем, а общая эффективность совместной работы мишени и электроники определяется количеством отдельных элементов изображения на строку сканирования (суммарное разрешение, эквивалентное количеству точек, образующих фотографии в газете, на ширине строки).

Считается, что изображение в системах наружного обзора имеет достаточно хорошее качество, если можно отличить человека от любого другого объекта и решить, была тревога ложной или настоящей.

Помимо необходимости идентификации следующим важным фактором при выборе камеры является выбор сочетания освещения и типа мишени камеры. Чувствительность мишени монохроматических камер к различным цветам освещения зависит от ее типа, поэтому тип используемой мишени должен соответствовать освещению, и наоборот.

Однако, очевидно, в некоторых ситуациях, в которых необходимо, чтобы нарушитель не знал о ведущемся за ним наблюдении, просматриваемое пространство должно быть освещено инфракрасным светом. Глаз человека не воспринимает этот свет, однако мишени камер могут быть сконструированы для регистрации света именно в этом диапазоне.

Одним из важнейших факторов для проектировщика системы является размер экрана монитора. Основная проблема заключается в том, что при

уменьшении размера экрана монитора размер движущейся светящейся точки, формирующей изображение, не может быть уменьшен в такой же пропорции.

Эта проблема вытекает из сочетания ограничений на фокусировку, ореол и материал экрана. При этом часть информации, достигающей монитора, теряется при формировании изображения на экране. Эти проблемы почти полностью решаются за счет использования более крупных экранов так, чтобы вся полученная информация была отображена на мониторе.

При дальнейшем увеличении размеров экрана светящаяся точка опять-таки не увеличивается в той же пропорции, поэтому линии на экране и промежутки между ними становятся более выраженными. Такие промежутки являются фактически неиспользуемым пространством и могут препятствовать восприятию изображения на экране.

Еще одним существенным фактором является расстояние от наблюдателя до экрана. Было установлено наиболее удобное расстояние от зрителя до экрана, а после этого был определен минимальный угол зрения до появления усталости. В результате был найден размер экрана, после чего была разработана электронная схема, обеспечивающая оптимальное разрешение для этого размера экрана.

Оптимальные размеры экрана по диагонали варьируются от 9 до 17 дюймов.

Четкость и яркость изображения наблюдаемого оператором на экране монитора, зависит от степени освещенности объектов наблюдения. В дневное время, особенно в солнечную погоду четкую картинку получить гораздо легче, чем в пасмурную. Для того, чтобы уравнять условия освещенности в разное время суток и при разных погодных условиях необходимо предусмотреть наличие искусственного освещения.

Оптимальное использование имеющегося света достигается при использовании видеокамер, оснащенных мишенями, предназначенными для низких уровней освещенности. Высокая чувствительность таких мишеней позволяет использовать их в условиях сумеречного освещения, после чего нужен уже искусственный свет, но все равно не в таком количестве, как для обычных камер.

Новая камера с чувствительной мишенью стоит дороже, чем уже бывшая в употреблении, поэтому следует найти компромисс между более высокой начальной и более низкой эксплуатационной стоимостью. Для достижения этого компромисса можно подключить систему искусственного освещения таким образом, чтобы она включалась только по команде системы обнаружения нарушителя одновременно для отпугивания и для освещения поля зрения видеокамеры.

Когда высокочувствительные камеры используются в таких разнообразных условиях освещения – от яркого солнечного до искусственного – во избежание ослепления и перегрузки камеры, необходимо автоматическое управление потоком света, попадающим в камеру.

Оно достигается за счет уменьшения поступающего потока света до минимального уровня, при котором камера может удовлетворительно работать,

а для этого, в свою очередь, используется автоматическая диафрагма, которая "затеняет" линзы точно так же, как в фотоаппарате. Если диафрагмы недостаточно для управления потоком света во всем рабочем диапазоне освещенностей, то используется дополнительное управление автоматическими фильтрами, которые помещаются в световой тракт между линзами и мишенью камеры при определенных уровнях освещения. Еще большее ослабление достигается с помощью автоматического управления усилением в электронных усилителях камеры.

Монтаж и эксплуатация видеосистем для работы внутри здания во многом аналогичны рассмотренным ранее. Общим для обоих вариантов фактором, который также следует учитывать это то, что по сравнению с человеческим глазом большинства объективов имеет более узкий угол обзора. Кроме того, человеческий глаз за счет подвижности еще более расширяет угол обзора и обладает способностью фокусироваться в течение доли секунды.

Обычно в установках видеонаблюдения задача расширения угла зрения решается за счет использования вращающегося в вертикальной и горизонтальной плоскостях корпуса, что позволяет видеокамере "смотреть" в нужном направлении под действием дистанционного управления.

Типовой поворотный механизм движется со скоростью 6 градусов за одну секунду – это означает, что для поворота на 60 градусов ему потребуется 10 секунд. Человеческий глаз делает то же самое менее, чем за одну секунду. Данное обстоятельство имеет большое значение при оценке надежности системы наблюдения, так как такой медленный поворот дает возможность злоумышленнику пересечь поле зрения, не попав в створ объектива, если он знает о технических характеристиках системы видеонаблюдения.

Кроме того, дежурный сотрудник службы безопасности помимо наблюдения за изображением на мониторах и управлением видеокамерами обычно выполняет и другие задачи, что еще в большей мере облегчает задачу злоумышленника.

В каждом конкретном случае разработчики должны объективно разобраться в вопросе, стоит ли устанавливать дорогостоящие системы наблюдения с изменяющимся углом поворота и наклона, или ограничиться установкой более дешевых камер с фиксированным направлением обзора.

Две разнесенные фиксированные камеры, направленные так, чтобы видеть не только то, что находится под ними и вокруг, но и в мертвых зонах друг у друга, в соединении с системой охранной сигнализации предоставляют наилучшую возможность наблюдения за всем, что происходит.

Ничто так не может сильнее поколебать уверенность человека в себе, как технические неясности, а это ведь может произойти именно в тот момент, когда человеку особенно нужна уверенность для принятия решения на основании того, что он видит на экране. Поэтому общая рекомендация – использовать в системах видеонаблюдения камеры с фиксированным направлением обзора с максимальным углом зрения, с высокочувствительными мишенями и с включением освещения по срабатыванию датчиков обнаружения нарушителя.

Поворот, наклон и увеличение должны использоваться, но скорее как исключения, а не как правило.

Альтернативой телевидению для наблюдения являются заслуживающие внимание фото- и кинокамеры с электронным управлением. Однако им трудно конкурировать с видеокамерами из-за необходимости проявлять отснятую пленку, что существенно увеличивает временной диапазон между фиксацией события и получением документальной информации.

Записанная видеоинформация не нуждается в дополнительной обработке, лучше защищена от повреждения и может быть воспроизведена непосредственно после записи. В результате этого видеозапись стала сейчас естественной частью систем видеонаблюдения, в особенности, когда видеокамеры используются непостоянно, например, при включении датчиков.

Центральной фигурой системы сигнализации должен быть сотрудник охраны, следящий за контрольным пультом. Поэтому предъявляются особые требования к уровню развития у него таких психических функций, как:

- внимание;
- устойчивость к монотонии;
- высокая самодисциплинированность и т.п.;

На нем лежит ответственность по принятию нужных действий в нужное время. Он должен уметь быстро оценивать визуальную информацию и принимать адекватные решения.

4.3. Видеокамеры в охранном телевидении

Самый первый и наиболее важный элемент системы охранного телевидения — это элемент, формирующий изображение, то есть видеокамера.

Термин «камера» произошел от латинского camera obscura, что означает «темная комната».

4.3.1. Видеокамеры с передающими трубками

Первые эксперименты с телевизионными камерами состоялись в 1930-х и были проведены инженером русского происхождения Владимиром Зворыкиным (Zworykin) (1889-1982). Первые камеры изготовлялись из стеклянных трубок и светочувствительного люминофорного покрытия на внутренней поверхности стекла. Сегодня мы называем их передающими трубками.

Работают передающие трубки по принципу фоточувствительности**,** основанному на фотоэффекте. Свет, проектируемый на люминофорный слой трубки (называемый мишенью) обладает энергией, достаточной, чтобы вызвать выбивание электронов из кристаллической решетки люминофора. Число выбиваемых электронов пропорционально свету, и таким образом формируется электрическое представление световой проекции. При появлении охранного телевидения существовало два основных типа трубок: видиконы и ньювиконы. Видикон был дешевле и менее чувствителен. Видиконы работали только с объективами с ручной установкой диафрагмы. Минимальная освещенность, необходимая для того, чтобы черно-белый видикон сформировал ви-

деосигнал, составляла порядка 5-10 лк, отраженных от объекта, при использовании объектива F/1.4.

Видеокамеры типа ньювикон были более чувствительны (до 1 люкса), более дорогие и требовали объективов с автодиафрагмой. Внешне они выглядели так же, как и видиконы, так что на вид их различить было непросто. Только опытный специалист по охранному телевидению мог заметить небольшие отличия в цветах области мишени: у видикона есть темно-фиолетовая составляющая, а у ньювикона – темно-синяя. Два типа видеокамер управляются различной электроникой, а видеокамеры типа ньювикон снабжены разъемом автодиафрагмы.

Работа всех передающих трубок основывается на принципе сканирования электронным лучом мишени внутри трубки под действием электромагнитного поля. Луч отклоняется электромагнитным полем, генерируемым электронной системой камеры. Чем больше света достигает светочувствительного слоя мишени, тем ниже ее сопротивление в этом месте. При проецировании изображения, благодаря фотоэффекту, формируется потенциальный рельеф. Когда анализирующий электронный луч сканирует фоточувствительный слой, он нейтрализует положительные заряды, так что по локальным сопротивлениям протекает ток. Когда электронный луч попадает в конкретную часть потенциального рельефа, электрический ток теряет заряд пропорционально количеству света. Этот очень слабый ток подается на видеоусилитель с очень высоким входным сопротивлением, который и формирует напряжение видеосигнала. В трубке должен быть тонкий и однородный фотослой – это очень важно. Этот слой порождает так называемый теневой ток, который существует даже тогда, когда объектив не проецирует изображение (диафрагма закрыта).

Функционирование передающих трубок опирается на несколько важных концепций.

Первое: большие габаритные размеры видеокамеры как таковой – стеклянная трубка, окружающая ее электромагнитная отклоняющая система и размеры электронных компонент системы – все это делало видеокамеры довольно громоздкими.

Второе: необходимость в использовании точного отклоняющего электромагнитного поля, которое заставляет электронный луч сканировать область мишени согласно телевизионным стандартам. Использование электромагнитной системы для сканирования означает, что внешние электромагнитные поля других источников могут влиять на процесс сканирования, вызывая искажения картинки.

Третье: необходимость высокого напряжения (до 1000 В) для придания ускорения электронному лучу и задания его траектории. Поэтому в видеокамерах приходится использовать высоковольтные компоненты, что всегда представляет собой потенциальную проблему для устойчивости электронных схем. Старые и высоковольтные конденсаторы могут начать подтекать, влага может создать токопроводящий воздушный слой вокруг компонент и привести к возникновению искровых разрядов.

Четвертое: необходимость наличия люминофорного слоя на мишени, который преобразует световую энергию в электрическую информацию. Люминофор постоянно подвергается электронной бомбардировке, и слой со временем изнашивается. Срок службы люминофорного покрытия трубки ограничен. При постоянной эксплуатации видеокамеры (как это и происходит в системах охранного телевидения) реальный ресурс видеокамеры составляет пару лет, после этого срока изображение начинает ослабевать, вследствие выжигания люминофора могут появиться «впечатанные» изображения – если видеокамера постоянно направлена на один и тот же объект. В результате мы можем увидеть такую картину: движущиеся люди похожи на призраков, они полупрозрачны и сквозь них просвечивают «впечатанные» изображения.

Пятое: **геометрические искажения,** обусловленные тем, что луч падает на мишень под различными углами; эта черта принципиально отлична от используемых сегодня ПЗС-видеокамер (и ее следует рассматривать как недостаток) и является врожденным свойством, наследуемым от конструкции трубки как таковой. В частности, траектория электронного луча короче, когда он попадает в центр мишени, по сравнению с его траекторией при сканировании краев. Поэтому возникают геометрические искажения проецируемого изображения. Во многих конструкциях введены магнитные и электронные системы коррекции таких искажений, но при каждом перемещении трубки приходится заново регулировать настройки.

4.3.2. ПЗС-видеокамеры

Новая ПЗС-технология позволила исключить все эти проблемы. Вначале микроэлектронная технология была не в состоянии создать элемент изображения (пиксел) на ПЗС-матрице меньший, чем поперечное сечение электронного луча. Это означает, что на заре технологии ПЗС-матриц их разрешение значительно отставало от разрешения трубок. Однако очень скоро удалось повысить разрешение ПЗС-матриц, так что оно стало сравнимо с качеством видеокамер с передающими трубками.

В 1970-х, когда появились первые персональные компьютеры, начались эксперименты с полупроводниковыми электронными компонентами – **приборами с зарядовой связью** – которые вначале предполагалось использовать в качестве запоминающих устройств. Очень скоро выяснилось, что ПЗС очень чувствительны к свету, и поэтому их лучше и эффективнее использовать в качестве светоприемников, а не в качестве запоминающих устройств. Основной принцип работы ПЗС заключается в сохранении информации электрических зарядов в фотоэлементах, а затем, когда потребуется, передаче этих зарядов на выходной каскад.

Итак, зарядовые пакеты – как только они сформировались в фотоэлементах матрицы – «стекают» на выходной каскад при использовании методов зарядовой связи. Таким образом электрическая связь обеспечивается управлением напряжением и временем для каждой ячейки, называемой элементом изображения (пиксел). Один из пионеров ПЗС-технологии, Гильберт Амелио, в своей ста-

тье, написанной в 1974 г., описывает зарядовую связь как «коллективный перенос всего мобильного электрического заряда, хранящегося на элементе полупроводниковой памяти на аналогичный сопряженный запоминающий элемент путем внешнего воздействия напряжением. Количество хранимого в мобильном пакете заряда может меняться в широких пределах в зависимости от приложенного напряжения и емкости запоминающих элементов. Величина электрического заряда в каждом пакете может представлять информацию».

ПЗС-чип может иметь либо линейную форму (линейный ПЗС), либо форму двумерной матрицы (ПЗС-матрица). Важно понимать, что они состоят из дискретных элементов (пиксел), но ПЗС-устройства не являются цифровыми устройствами. Каждый пиксел может содержать любое число электронов, пропорциональное падающему на него свету, таким образом представляя аналоговую информацию.

Дискретные пакеты электронов переносятся (если время экспонирования закончилось) одновременным сдвигом рядов и столбцов пакетов на внешний каскад чипа.

Поэтому ПЗС-матрицы по сути своей являются светочувствительными аналоговыми сдвиговыми регистрами.

Сегодня ПЗС не используются в качестве запоминающих устройств, а только в качестве фотоприемников. Их можно найти во многих устройствах, с которыми мы сталкиваемся каждый день: в факсимильных аппаратах, сканерах используются линейные ПЗС; во многих фотокамерах с автофокусом используются ПЗС-чипы автофокусировки; в географическом аэромониторинге, космическом зондировании планеты, промышленном обследовании материалов тоже применяются камеры с линейными ПЗС, и наконец, хотя это и не последнее, многие современные телевизионные камеры, как в широком телевещании, так и в системах охранного телевидения, используют ПЗС-чипы.

ПЗС-видеокамеры обладают многими преимуществами (конструктивными) перед видеокамерами с передающими трубками, хотя, как ранее упоминалось, поначалу возникали трудности с разрешающей способностью. В наши дни технология достигла такого уровня, что высокое разрешение больше не проблема.

Вот основные преимущества ПЗС-видеокамер в сравнении с видеокамерами на передающих трубках:

- очень низкая минимальная освещенность (для черно-белых до 1 лк на объекте);
- отсутствие геометрических искажений благодаря точной двумерной конструкции;
- низкое энергопотребление;
- не требуется высокое напряжение для ускорения луча;
- маленькие размеры;
- не подвержены воздействию внешних электромагнитных полей;
- и самое важное неограниченное время жизни электронов, генерируемых фотоэффектом.

Основная классификация ПЗС-матриц – это деление на линейные и двумерные матрицы. Линейные чипы используются в тех случаях, когда объекты движутся только в одном направлении (как в факсимильных аппаратах и сканерах).

В охранном телевидении нас интересуют только двумерные матрицы, так называемые матрицы размеров 2/3", 1/2", 1/3". Эти размеры не представляют диагональные размеры матриц, а соответствуют диаметрам передающих трубок, дающих такое же изображение.

4.3.3. Технические параметры видеокамер и что они означают

Основные задачи видеокамеры — захват изображений, разбиение их на ряд неподвижных кадров и строк, передача и быстрое воспроизведение на экране, в результате чего человеческий глаз воспринимает их как движущееся изображение. Выбирая видеокамеру, мы должны принимать во внимание ряд характеристик. Некоторые из них очень важны, другие не очень, все зависит от применения.

Рассмотрим некоторые наиболее важные характеристики:

- чувствительность видеокамеры;
- минимальная освещенность;
- разрешающая способность видеокамеры;
- отношение сигнал/шум;
- динамический диапазон.

Другие, менее важные, но тоже имеющие значение характеристики включают: гамма-коррекцию, темновой ток, спектральную чувствительность, оптическую низкочастотную фильтрацию, диапазон АРУ в дБ, энергопотребление, габаритные размеры и пр.

Чувствительность характеризуется минимальным отверстием диафрагмы (максимальным F-числом), дающим видеосигнал полного размаха 1 В на тестовой таблице, освещенность которой равна точно 2000 лк и создана источником с цветовой температурой 3200° К.

В охранном телевидении не существует четкого определения минимальной освещенности, в отличие от чувствительности видеокамеры. Обычно этот термин относят к наименьшей освещенности на объекте, при которой данная видеокамера дает распознаваемый видеосигнал. Поэтому данная характеристика выражается в люксах на объекте, при которых получается данный видеосигнал.

Разрешающая способность по вертикали — это максимальное число горизонтальных линий, которое способна передать видеокамера. Это число ограничено стандартом CCIR/PAL до 625 горизонтальных строк и стандартом EIA/NTSC до 525 строк.

Разрешающая способность по горизонтали — это максимальное число вертикальных линий, которые способна передать видеокамера (в тех случаях, когда в документации указано только разрешающая способность, то это надо понимать, как разрешающая способность по горизонтали). Это число

ограничено только технологией и качеством монитора. В наши дни существуют ПЗС-видеокамеры с разрешающей способностью по горизонтали более 600 ТВЛ.

Горизонтальное разрешение ПЗС-видеокамер обычно равно 75% горизонтальных пиксел ПЗС-матрицы. Как объяснялось выше, это результат соотношения сторон 4:3. В частности, подсчитывая вертикальные линии в целях определения горизонтального разрешения, мы считаем только горизонтальную ширину, эквивалентную высоте монитора по вертикали.

Отношение сигнал/шум показывает, насколько хорош может быть видеосигнал видеокамеры, особенно в условиях низкой освещенности. Шума избежать невозможно, но его можно минимизировать. В основном, он зависит от качества ПЗС-матрицы, электроники и внешних электромагнитных воздействий, но также в сильной степени и от температуры электроники. Металлический корпус видеокамеры в значительной степени защищает от внешних электромагнитных воздействий. Источниками шума внутри видеокамеры являются как пассивные, так и активные компоненты, поэтому «зашумленность» зависит от их качества, конструкции системы и в сильной степени от температуры. Вот почему, указывая отношение сигнал/шум, производитель должен также указать и температуру, при которой проводились измерения.

Шум в изображении аналогичен по природе шуму в аудиозаписях. На экране зашумленное изображение дает зернистость или снег, а на цветном изображении могут быть цветовые вспышки. Сильно зашумленные видеосигналы бывает трудно синхронизировать, изображение может получиться нечетким, с плохим разрешением. Зашумленное изображение от видеокамеры становится еще хуже при уменьшении освещенности объекта.

Отношение сигнал/шум выражается в децибелах (дБ). Децибелы – это относительные единицы. Отношение выражается не в виде абсолютной величины, а в форме логарифма. Причина проста: логарифмы позволяют переводить большие отношения чисел к двух-трехзначным числам, но что более важно, преобразование сигнала (при вычислении затухания или усиления системы) сводится к простому сложению или умножению. Другая причина использования децибел (т.е. логарифма) — это более естественное понимание уровня звука и изображения. В частности, ухо человека воспринимает звук, а глаз воспринимает свет, подчиняясь логарифмическому закону.

Динамический диапазон нечасто упоминается в технических характеристиках видеокамер охранного телевидения. Однако, это очень важная деталь, характеризующая эффективность камеры. Динамический диапазон ПЗС-матрицы определяется как максимальный сигнал накопления (насыщенная экспозиция), деленный на общее среднеквадратическое значение шума эквивалентной экспозиции. Динамический диапазон аналогичен отношению сигнал/шум, но относится только к динамике ПЗС-матрицы при обработке темных и ярких объектов в пределах одной сцены. Отношение сигнал/шум относится к полному сигналу, включая электронные схемы видеокамеры, и выражается в дБ, а динамический диапазон – это отношение, не логарифм.

4.4. Видеомониторы

Часто видеомониторы считают незначительным компонентном охранного телевидения в сравнении с другими составляющими системы. Однако, если качество видеомонитора не эквивалентно качеству видеокамеры (или хуже), то общее качество видеосистемы будет снижено.

Видеомонитор воспроизводит поступающий с видеокамеры сигнал после того, как он пройдет через средства передачи видеосигналов и устройства коммутации. Видеокамера может быть высочайшего качества, с высокой разрешающей способностью, но если видеомонитор не способен воспроизвести сигнал равным или лучшим образом, то вся система потеряет в качестве.

В охранном телевидении, также как и в телевещании, большинство видеомониторов выполнено на кинескопах, т.е. устройствах, действующих на основе технологии электроннолучевых трубок, которые преобразуют электрическую информацию видеосигнала в визуальную. Сегодня существует множество альтернатив кинескопам: жидкокристаллические мониторы (ЖК), плазменные панели, проекционные и т.п., но наиболее популярны все же видеомониторы на кинескопах. Изнутри экран кинескопа покрыт слоем люминофора, в котором при бомбардировке электронным лучом происходит преобразование кинетической энергии электронов в световое излучение.

Видеомониторы в охранном телевидении подразделяются на две основные группы: черно-белые и цветные. По рекомендациям ТВ-стандартов между черно-белыми и цветными видеомониторами должна сохраняться совместимость. Другими словами, черно-белый видеосигнал может быть воспроизведен на цветном видеомониторе, а цветной сигнал – на черно-белом видеомониторе. Черно-белые видеомониторы характеризуются более высокой разрешающей способностью (поскольку имеют одно непрерывное люминесцентное покрытие), а цветные видеомониторы дают ценную информацию о цветах объектов. Какой фактор более важен – зависит от применения. Например, для видеосистемы распознавания номерных знаков важнее высокое разрешение, и поэтому лучшим выбором будет черно-белая видеосистема камера/монитор, а в других случаях, когда, скажем, требуется идентификация личности, лучше выбрать цветную видеосистему.

Видеомониторы характеризуются размерами диагонали экрана, обычно выраженными в дюймах, иногда в сантиметрах. Черно-белые видеомониторы бывают самых разных размеров, чаще всего используются 9" (23 см) и 12" (31 см). Видеомониторы меньших размеров – 5" (13 см) и 7" (18 см) – не очень удобны, за исключением разве что систем заднего обзора, видеопереговорных систем, а также для регулировки заднего фокуса объективов. Большие мониторы чаще всего используются с видеомультиплексорами.

Число видеомониторов в системе охранного телевидения может быть довольно большим. Проектируя систему, важно знать, сколько видеомониторов можно будет использовать на месте, как их расположить и пра-

вильно выбрать расстояние просмотра. Есть ряд факторов и рекомендаций даже для системы с одним видеомонитором. Это особенно важно, если операторы проводят большую часть времени перед экранами видеомониторов.

В рекомендации охранного телевидения говорится, что предпочтительные условия просмотра зависят от частоты полей ТВ-системы, размера экрана и соотношения между расстоянием просмотра и размерами экрана. Важно также спланировать количество операторов для наблюдения за данным числом видеомониторов и точки наблюдения. Известно, что дрожание по вертикали становится особенно заметным в периферической области зрения. Другими словами, если перед вами много видеомониторов, то скорость обновления кадров окружающих видеомониторов влияет на ваше зрение, даже если на видеомонитор, находящийся прямо перед вами, вам смотреть вполне комфортно. Поэтому некоторые производители разрабатывают для охранного телевидения 100 Гц видеомониторы (это более критично для PAL и SECAM из-за их более низкой частоты кадровой развертки). 100 Гц видеомониторы просто удваивают скорость обновления в 50 полей, и изображение выглядит неподвижным «как скала». Сидеть перед такими видеомониторами длительное время определенно лучше.

Рассмотрим еще один вопрос: электростатическое излучение больших видеомониторов. Хотя оно и пренебрежимо мало, но если в помещении находится видеостена, то большое количество мониторов может оказывать заметное влияние на среду. Это подтверждает и количество пыли, собираемой большим числом видеомониторов. В медицине принят стандарт низкого уровня радиации – MPR II. Некоторые производители тоже приняли этот стандарт и будут отдавать предпочтение системам с такими видеомониторами.

В больших системах управление визуальным воспроизведением имеет жизненно важное значение. Например, не все видеомониторы должны воспроизводить изображение все время. Эффективность системы будет выше, если оператор(ы) будет(ут) концентрировать внимание на одном или двух активных мониторах (обычно большего размера), а остальные будут погашены. В случае активности (при обнаружении тревоги), детектирования движения или пропажи видеосигнала, погашенный видеомонитор может быть запрограммирован на вывод изображения предварительно выбранной видеокамеры. В этом случае внимание оператора будет сразу же привлечено к новому изображению, и система будет более эффективной. Дополнительным преимуществом станет увеличение срока службы видеомонитора. Многие матричные видеокоммутаторы могут быть запрограммированы на гашение и вывод изображения с видеокамеры по тревоге, только когда это необходимо.

Жидкокристаллические мониторы (ЖК-мониторы) все еще находятся на раннем этапе использования в охранном телевидении. Они становятся все более популярны в ноутбуках, хотя могут использоваться и в охранном телевидении. Принцип функционирования ЖК отличается от принципов ЭЛТ.

Изображение формируется не сканирующим электронным лучом, а путем адресации жидкокристаллических ячеек, которые поляризуются в различных направлениях, когда к их электродам прикладывается напряжение. Величина напряжения определяет угол поляризации, что в свою очередь определяет прозрачность каждого пикселя, формируя таким образом элементы видеоизображения. Преимущества ЖК-видеомониторов: нет необходимости в элементах высокого напряжения; нет слоя люминофора, т.е. срок службы экрана неограничен; плоский экран и миниатюрные габариты; нет геометрических искажений; низкое энергопотребление; нет влияний электромагнитных полей, как у кинескопов и пр.

Есть несколько вариаций ЖК-технологий. Один из хорошо известных типов ЖК-устройств – это так называемые пассивные ЖК-мониторы, кристаллическая матрица которых состоит из пассивных жидких кристаллов, которые поляризуются в зависимости от приложенного напряжения. Другая, более продвинутая технология, использует тонкие пленочные транзисторы в каждой ЖК-ячейке, а так как транзисторы являются активными компонентами, такая технология называется «активной матричной ЖК (TFT LCD) панелью».

Основной недостаток — изображение формируется отраженным светом, а не генерируемым, как у кинескопов. Некоторые ЖК-панели, особенно цветные, используют область встречной подсветки, но это все же отличается от генерации света в кинескопе. Другой недостаток – это эффект «смазывания» из-за медленного пиксельного отклика на процесс строчной развертки, выглядит он как вертикальный ореол. И наконец, размеры пикселя определяют максимальную разрешающую способность, а она ограничена развитием ЖК-технологии. За счет уменьшения размеров ЖК-дисплеев легко достигается разрешение уровня S-VGA, но, как мы видим на примере компьютерной индустрии, увеличение общих размеров таких дисплеев весьма затруднительно из-за задержек очень быстрых сигналов управления, адресуемых к каждому пикселю. Каждый день появляются новшества и вариации в ЖК-материалах, используемых в ЖК-технологии. Следует ожидать, что рано или поздно такие дисплеи станут неотъемлемой частью охранного телевидения.

Проекционные видеомониторы используются для формирования больших изображений. Несколько лет назад проекционные видеомониторы были очень громоздкими, дорогими и сложными в использовании и установке. Сегодня видеопроекторы гораздо меньше, дешевле, имеют большую яркость и проще в использовании и установке. Большинство проекторов — это однообъективные цветные проекторы, фильтрующие свет через ЖК-пленку. Проектор не может давать такую же яркость, как и кинескоп, но технология развивается очень быстро, и на рынке появляются все более и более яркие проекторы.

Довольно часто требуется, чтобы видеосигнал проецировался на большой экран. В рамках современных технологий созданы системы охранного телевидения широкого использования (например, в торговых центрах): в таких системах изображение с видеокамер выводится на большой экран,

доступный для просмотра многим людям. До настоящего времени это обычно делалось при помощи трех проекторов (RGB) или видео-стены, составленной из 4x4 или 5x5 видеомониторов. Позже стали появляться проекторы с цветными ЖК-фильтрами. Такие типы проекторов громоздки, дороги, дают не очень яркое изображение с не очень высоким разрешением. Одна из идей, разработанных в Texas Instruments™, может удовлетворить всем вышеперечисленным требованиям — это технология DMD, цифровые микрозеркальные устройства. Концепция DMD основана на микросхеме памяти с матрицей, состоящей из миллионов микрозеркал (похожей по размерам и виду на ПЗС-матрицу). Источник света проецирует изображение на DMD-чип, а зеркала отражают изображение на экран любого размера. Размер каждого зеркала – 26 миллионных миллиметра. Зеркала так малы, что в крупице соли могут поместиться сотни зеркал. Каждое зеркало представляет пиксель экрана. Все они контролируются, включаются и выключаются схемой, расположенной на матрице, и каждое из сотен переключений в секунду выполняется с огромной точностью. Зеркала запрограммированы на сохранение определенного угла отражения для различных временных периодов в пределах одного кадра. Это позволяет создать проекцию градаций яркостей или дать корректное представление цвета. Самое главное преимущество таких устройств (кроме миниатюрных физических размеров) – это в равной степени высокое разрешение, яркость и точность цветопередачи, не зависящие от размеров экрана.

Плазменные видеомониторы состоят из массивов пикселей, каждый из которых включает группу из трех люминофоров: красного, зеленого и синего. В противоположность кинескопам, где световое излучение вызвано электронной бомбардировкой, в плазменных панелях газ, находящийся в плазменном состоянии, реагирует с люминофором каждого элемента пикселя. В плазменных панелях каждый подпиксел контролируется индивидуально, что позволяет получить 16,7 млн цветов. Благодаря тому факту, что каждый пиксель возбуждается индивидуально, не происходит геометрических искажений, как в кинескопе, а четкость изображения и богатство цветов поднимаются на новые уровни. Контрастность картинки тоже высока, обычно более 400:1, что делает плазменные панели пригодными для ярко освещенных зон.

Так как плазменная панель не требует высоких напряжений (как кинескоп), то возможно увеличение размеров дисплеев. Типичный размер плазменной панели лежит в пределах от 105 см (42") до 125 см (50"). Но самое важное, что толщина плазменных панелей очень мала – от 10 до 15 см (4-6"). Это не только привлекательно с эстетической точки зрения, но и очень удобно для помещений с ограниченным пространством.

Следует отметить, что поскольку работа плазменных панелей основывается на люминофоре, то они со временем выцветают. Производители обычно говорят о 30000 часах работы, после чего яркость снижается до 50% своей начальной величины. Это порядка трех лет непрерывной работы, примерно столько же работают видеомониторы с кинескопами.

Недавно Motorola™ представила еще одну альтернативу отличного воспроизведения, но на экране стандартного размера, а не на проекционном экране. Концепция плоского дисплея с активной эмиссией света получила название «технология FED» (дисплей с автоэлектронной эмиссией). Вместо одного катода (как в случае стандартного дисплея с кинескопом), в FED-устройствах на каждый пиксель приходятся сотни маленьких источников катодных лучей. FED-панель состоит из двух стеклянных пластин, разделенных вакуумом. Заднее стекло (катод) создано из миллионов мельчайших вершинок, источников электронов, ускоряющихся в вакууме. Переднее стекло (анод) покрыто слоями стандартных люминофоров.

FED-панель обладает многими преимуществами анодного стекла кинескопа, но она тоньше, легче, потребляет меньше энергии и не дает геометрических искажений. Компании, разрабатывающие FED-устройства, утверждают, что эти типы панелей будут дешевле, так как их проще изготавливать, чем ЖК-панели; а поскольку FED-панели не нуждаются в единой RGB-пушке (которая и определяет размеры и форму кинескопа), то они будут больше, но тоньше и легче.

4.5. Устройства обработки видеосигналов

Простая концепция «камера-монитор» используется только в небольших системах охранного телевидения. В более крупных системах сигнал до воспроизведения на видеомониторе проходит через видеокоммутатор или другое оборудование, осуществляющее обработку видеосигнала.

Термин «устройство обработки видеосигналов» относится к любому электронному устройству, выполняющему ту или иную обработку видеосигнала: переключение между несколькими входами', сжатие на один квадрант экрана, подъем высоких частот и др.

4.5.1. Аналоговое коммутационное оборудование

Самое простое и наиболее широко распространенное устройство, используемое в небольших и средних видеосистемах, — это последовательный видеокоммутатор. Поскольку в большинстве систем охранного телевидения видеокамер больше, чем видеомониторов, то требуется устройство, последовательно переключающееся с сигнала одной видеокамеры на сигнал другой. Такое устройство называется последовательным видеокоммутатором.

Последовательные видеокоммутаторы бывают разные. Самый простой – это 4-входовый видеокоммутатор, есть 6, 8, 12, 16 и даже 20-входовые видеокоммутаторы.

На передней панели видеокоммутатора расположен ряд кнопок для каждого входа, и кроме переключателя для ручного выбора видеокамер есть переключатель для включения видеокамер в последовательность или их обход. При помощи переменного резистора может быть изменено время наблюдения. Наиболее распространенная и целесообразная установка времени наблюдения составляет 2-3 секунды. Более короткое время слишком непрактично и будет

утомлять глаза оператора, а более длительное время сканирования может привести к потере информации с тех видеокамер, которые не отображались в это время на экране.

Кроме классификации по количеству видеовходов, последовательные коммутаторы можно классифицировать по наличию или отсутствию входов тревоги. Если последовательный видеокоммутатор имеет входы тревоги, это означает, что срабатывание внешних нормально разомкнутых (N/O) или нормально замкнутых (N/C) «сухих» контактов может остановить последовательное переключение и отобразить на экране видеосигнал из зоны тревоги. В качестве источников сигнала тревоги могут служить различные устройства тревожной сигнализации.

Последовательный видеокоммутатор (или для краткости коммутатор) – это самое экономичное устройство в цепи между совокупностью видеокамер и видеомонитором. Это не значит, что не существует более сложных и усовершенствованных последовательных коммутаторов. Существуют модели с функцией генератора текста (идентификация видеокамер, время, дата), множественными опциями конфигурации интерфейса RS-485 или RS-422 и пр.

Матричный видеокоммутатор (Video Matrix Switcher – VMS) приходится старшим братом последовательному коммутатору. Матричный видеокоммутатор (VMS) является мозгом системы и входит в состав больших систем охранного телевидения.

Если мы расположим на схеме видеовходы против видеовыходов, то получим матрицу — отсюда и название «матричный». Довольно часто матричные видеокоммутаторы называют узловыми (cross-point). Узлы (или точки пересечения) — это электронные переключатели, которые в любой момент могут подключить любой вход к любому выходу, сохраняя при этом режим согласования нагрузки. Так, один видеосигнал может быть выбран одновременно более чем на одном выходе. А несколько входов могут быть выбраны для переключения по одному выходу, только в этом случае мы получим последовательное переключение между несколькими входами, так как иметь более одного видеосигнала на одном выходе в один момент времени невозможно.

Таким образом, матричный видеокоммутатор по существу представляет собой большой последовательный коммутатор с рядом усовершенствований. VMS может контролироваться несколькими операторами. В этом случае каждый оператор обычно контролирует один видеоканал. В зависимости от модели VMS может быть достигнут определенный уровень интеллектуального управления. Операторы могут иметь равные или различные приоритеты, зависящие от их положения в структуре безопасности.

VMS обрабатывают сигналы со многих видеовходов и подают их на большое число выходов, но, что наиболее важно, их число может быть легко расширено просто добавлением модулей.

В состав VMS входят цифровые контроллеры для управления поворотными устройствами и объективами.

VMS имеет множество входов и выходов тревоги и может быть расширен до практически любого их количества. Возможна любая комбинация тревог, вроде N/O (нормально разомкнутые контакты), N/C (нормально замкнутые контакты) и их логические комбинации OR (ИЛИ), NOR (ИЛИ-НЕ).AND(M), NAND(M-НЕ).

Мозгом устройства является микропроцессор, его использование позволяет матричным видеокоммутаторам выполнять сложные задачи по управлению видеосигналом и сигналами тревоги.

4.5.2. Цифровое переключение и оборудование для обработки видеосигнала

«Неумение» последовательных коммутаторов отображать все видеокамеры одновременно и проблемы с синхронизацией заставили разработчиков оборудования для систем охранного телевидения на создание нового устройства – видеоквадратора (разделителя экрана).

Видеоквадратор помещает изображение от четырех (или менее) видеокамер на один экран, разделенный на четыре прямоугольные области, по аналогии с прямоугольной системой координат иногда называемые квадрантами (отсюда иногда используемое название такого прибора «quad»). Для решения этой задачи видеосигнал вначале должен быть оцифрован, а затем сжат до размера соответствующего квадранта (отсюда еще одно название прибора — quad compressor). Электроника прибора приводит все синхроимпульсы к единой временной базе, в результате формируется единый видеосигнал, в котором представлены сигналы всех четырех квадрантов, поэтому нет необходимости во внешней синхронизации.

Видеоквадратор – это прибор с аналоговыми входом и выходом, выполняющий цифровую обработку изображения.

Важный аспект видеоквадратора — это время обработки изображения. Когда появились первые устройства, цифровая электроника работала сравнительно медленно, и видеоквадратор мог обрабатывать всего несколько изображений в секунду, поэтому вы могли видеть «дерганье» перемещающихся объектов на экране. Медленные видеоквадраторы есть и сегодня. Чтобы движение на экране было плавным, электроника должна обрабатывать каждое изображение на полевой частоте ТВ-системы (1/50 с или 1/60 с), только тогда на отображении не будет задержек и эффект оцифровки будет менее заметен. Такие «быстрые» приборы называются видеоквадраторами реального времени. Видеоквадраторы реального времени с высоким разрешением стоят дорого. Цветные приборы дороже, чем черно-белые, так как в этом случае на каждый канал требуется три модуля кадровой памяти (по числу первичных цветов). Если в системе больше четырех видеокамер, то решением может быть использование двухстраничных видеоквадраторов, в этом случае до 8 видеокамер могут переключаться последовательно в виде двух изображений с квадовым представлением. Большинство таких видеоквадраторов позволяет настраивать время отображения между переключениями.

Другая очень удобная характеристика, свойственная большинству видеоквадраторов, — это входы тревоги. При получении сигнала тревоги, соответствующая видеокамера переключается с квадового режима на полноэкранный. Обычно это режим реального времени, то есть аналоговый сигнал отображается без цифровой обработки и хранения в кадровой памяти. В качестве устройств активации могут быть использованы самые разные датчики, но чаще всего это пассивные и активные инфракрасные детекторы, видеодетекторы движения, тревожные кнопки и датчики открывания дверей.

Естественная эволюция устройств цифровой обработки изображений сделала видеомультиплексоры лучшей альтернативой видеоквадраторам, особенно для записи. Видеомультиплексоры — это устройства, выполняющие временное мультиплексирование входных видеосигналов и дающие два типа выходных видеосигналов: один для просмотра и один для записи.

Выход для видеонаблюдения позволяет показывать изображения со всех видеокамер на одном экране одновременно. То есть, если у нас есть 9-канальный видеомультиплексор с 9 видеокамерами, то все они будут представлены на экране в виде мозаики 3x3. Та же концепция применима к 4- и 16-канальным видеомультиплексорам. В большинстве видеомультиплексоров любая видеокамера может быть выбрана для полноэкранного отображения. Пока на видеовыходе воспроизводятся эти изображения, на магнитофонный выход видеомультиплексора посылаются разделенные по времени мультиплексированные изображения со всех видеокамер, выбранных для записи. Это разделенное по времени мультиплексирование похоже на очень быстрый последовательный видеокоммутатор с той лишь разницей, что все видеосигналы синхронизированы для последовательной записи на видеомагнитофон. Некоторые производители изготавливают видеомультиплексоры, выполняющие лишь быстрое переключение каналов (для записи) и вывод полноэкранных изображений, без функции мозаичного воспроизведения. Такие устройства называются frame switcher (коммутатор кадров), причем при записи они ведут себя подобно видеомультиплексорам.

Вместо того, чтобы записывать одну видеокамеру несколько секунд, затем другую и т.д. (что делает последовательный видеокоммутатор), видеомультиплексор обрабатывает видеосигнал таким образом, что каждое следующее поле, посылаемое на видеомагнитофон, исходит от другой видеокамеры (обычно следующего по порядку входа). Итак, в действительности мы имеем на выходе очень быстро переключаемый сигнал, который переключается со скоростью, соответствующей скорости записывающих головок.

Если необходимо воспроизведение, то выход видеомагнитофона вначале обращается к видеомультиплексору, затем видеомультиплексор извлекает сигнал выбранной видеокамеры и посылает изображение на видеомонитор. Видеомультиплексор может отобразить любую видеокамеру на полном экране или воспроизвести все записанные видеокамеры в мозаичном режиме (вывести несколько изображений одновременно).

4.5.3. Видеодетекторы движения

Видеодетекторы движения (Video Motion Detector — VMD) — это устройства, анализирующие поступающие на вход видеосигналы и определяющие наличие изменений в видеосигнале; в случае их появления активируется выход тревоги.

На самом раннем этапе развития VMD была возможна только аналоговая обработка. Такие простые VMD все еще применяются и, пожалуй, достаточно эффективны в сопоставлении с их ценой, хотя они не способны сделать сложный анализ и поэтому дают большое количество ложных тревог. Принципы работы аналогового VMD (иногда их называют видеосенсорами движения) очень просты: видеосигнал с камеры подается на VMD и затем на монитор или любой видеокоммутатор. При помощи нескольких регуляторов, расположенных на передней панели устройства, на анализируемом изображении позиционируются маленькие метки (обычно четыре). Эти прямоугольные метки указывают зоны чувствительности, а уровень видеосигнала определяется электроникой VMD. Как только уровень меняется (становится выше или ниже) – то есть кто-то появился в поле зрения и попал в отмеченные зоны — активируется тревога. Ложные тревоги будут всегда – их могут вызвать колышущиеся на ветру деревья, прогуливающиеся кошки, световые блики – но причина тревоги всегда может быть определена при воспроизведении записи с видеомагнитофона (если VMD к нему подсоединен).

VMD нередко являются лучшим решением, чем пассивные инфракрасные детекторы (PIR), не только потому, что причину тревоги можно увидеть, но и потому, что VMD точно анализирует все, что видит видеокамера.

Следующий шаг VMD-технологии – это цифровой видеодетектор движения (DVMD), еще более сложное и популярное устройство. И конечно же, более дорогое, но при этом более надежное и дающее меньшее количество ложных тревог. В последние годы были разработаны DVMD-устройства, учитывающие перспективу. Это означает, что по мере передвижения объектов в направлении «от камеры» (при этом их размеры на изображении уменьшаются), увеличивается чувствительность VMD с целью компенсации уменьшения размеров объекта из-за эффекта перспективы.

Довольно часто более удобен такой вариант: детектирование тревоги происходит не в том случае, когда кто-то или что-то движется в поле зрения, а только когда фиксированный объект смещается со своего положения. Эти можно сделать при помощи видеодетектора стационарных объектов (VNMD, video non-motion detector). Это устройство во многом аналогично VMD, но только в этом случае собирается дополнительная информация о тех объектах, которые стационарны в течение длительного времени. Любые движения вокруг выбранных объектов не вызывают сигнала тревоги; тревога активируется только в том случае, когда защищаемый объект смещается со своей стационарной позиции.

В последние годы появились видеокамеры с цифровой обработкой сигнала со встроенной схемой VMD. Это удобно в тех системах, в которых за-

пись и/или тревога активируются только в том случае, если человек или объект перемещается в поле зрения данной видеокамеры.

4.6. Устройства видеопамяти

Концептуально устройство видеопамяти — это очень простое электронное устройство, предназначенное для временного хранения изображений. Две его основные части — это аналого-цифровой преобразователь и оперативное запоминающее устройство (RAM). Первая часть осуществляет преобразование аналогового видеосигнала в цифровой код, который затем сохраняется в ОЗУ до тех пор, пока подключено питание.

Главным преимуществом устройства видеопамяти в сравнении с видеомагнитофонами является время отклика. Так как устройство не содержит механических частей, то запись изображений при активации тревоги выполняется мгновенно. Затем информация передается на видеопринтер или видеомонитор для просмотра или проверки.

Более сложные устройства обычно содержат несколько страниц кадровой памяти, на которые постоянно записываются последовательности изображений на основе принципа «первым поступил — первым выводится» (FIFO), вплоть до момента активации тревоги. При активации тревоги можно просмотреть не только события, происходящие в момент тревоги, но также несколько кадров, предшествующих ситуации тревоги; таким образом устройство хранит краткую историю событий. Это та же концепция, что и «предыстория тревог» в VMD-устройствах.

Устройства видеопамяти, используемые в системах охранного телевидения, делятся на черно-белые и цветные устройства. Качество устройства видеопамяти определяется прежде всего разрешающей способностью, то есть количеством пиксел, которые могут быть сохранены, и, во-вторых, выраженным в двоичных единицах количеством уровней серого, а в случае цветного устройства – числом бит, используемых для хранения цвета. Типичное устройство видеопамяти хорошего качества имеет более 400x400 пиксел, а обычное разрешение составляет 752x480 пиксел и 256 уровней яркости (28). Для цветного устройства видеопамяти (с тремя цветовыми каналами) мы получим более 16 млн. цветов (256x256x256).

4.7. Устройства записи на диск (DVR)

Запись изображений на ленту кассетного видеомагнитофона сама по себе экономична, но страдает отсутствием ряда деталей, которые заставляют нас искать новые, как правило, цифровые методы хранения записи. Прежде всего, применение аналогового метода в видеомагнитофонах не позволяет осуществить прямой и быстрый доступ к желаемому кадру, если, конечно, не воспользоваться при этом подходящим режимом быстрого поиска записи по тревоге (доступным для большинства TL-видеомагнитофонов). В видеомагнитофонах информация хранится в аналоговом формате и не может быть впоследствии обработана. И, наконец, качество воспроизводимого изображения всегда ниже качества оригинального источника.

Ниже перечислены основные преимущества цифровой видеозаписи.

- Цифровые сигналы более устойчивы к шуму.
- Цифровые сигналы могут быть многократно перезаписаны с тем же самым превосходным качеством изображения, которое было достигнуто при первичной записи.
- Цифровые сигналы могут быть защищены от несанкционированного вмешательства («водяные знаки»).

Жесткие диски имеют намного более высокоскоростной выход, чем другие цифровые накопители информации, и качество изображения, превышающее S-VHS, может быть достигнуто без каких-либо проблем. Главное неудобство, связанное с жесткими дисками, – это то, что их емкость все еще недостаточна для записи продолжительностью в несколько дней, что реализуется при использовании TL-видеомагнитофонов. Однако существует хорошая и вполне разумная комбинация, когда жесткий диск, выступая в качестве первичного накопителя информации, достигнув своего заполнения, автоматически перегружает содержимое на резервные цифровые аудиокассеты (DAT), JAZ-привод, DVD-RAM, на ленту цифрового видео или на другие подобные носители большой емкости. Это резервное копирование может быть автоматизировано таким образом, что будет полностью исключено физическое вмешательство оператора. После этого жесткий диск может быть настроен на продолжение записи поверх ранее записанной видеоинформации (запись по циклу).

Накопители на жестких дисках характеризуются довольно быстрым доступом, и, применяя кэширование и сильное сжатие, можно восстановить изображения в режиме реального времени. Какое количество видеоизображений может храниться в памяти, зависит, в первую очередь, от способа сжатия и качества изображений, отобранных для этого сжатия, но, как правило, этого достаточно для работы множества видеокамер с превосходным качеством в режиме time lapse в течение более 24 часов.

4.8. Средства передачи видеосигнала

Изображение, зафиксированное объективом и видеокамерой и затем преобразованное в электрический сигнал, поступает на коммутатор, видеомонитор или записывающее устройство.

Для того, чтобы видеосигнал попал из пункта А в пункт Б, он должен пройти через передающую среду. То же самое относится к сигналу управляющих данных.

Самыми распространенными средствами передачи видеоинформации в охранном телевидении являются:

- коаксиальный кабель;
- кабель витой пары;
- микроволновая связь;
- радиочастотная передача (эфирная);
- связь с помощью инфракрасного излучения;
- телефонная линия;
- оптико-волоконный кабель.

Для видеопередачи чаще всего используется коаксиальный кабель, но все большую популярность приобретает волоконная оптика – благодаря ее превосходным характеристикам. Также можно использовать смешанные средства передачи, например, микроволновую передачу видеосигнала и передачу управляющих поворотным устройством и трансфокатором данных (PTZ-данных) через витую пару.

4.8.1. Коаксиальные кабели

Коаксиальный кабель — самое распространенное средство передачи видеосигналов, а иногда видео и PTZ-данных вместе. Такую передачу называют несимметричной передачей, исходя из концепции коаксиального кабеля.

Кабель имеет симметричное и соосное строение. Видеосигнал проходит через центральную жилу, в то время как экран используется для уравнивания нулевого потенциала концевых устройств – видеокамеры и видеомонитора, например. И не только для этого, экран также защищает центральную жилу от внешних нежелательных электромагнитных помех (ЭМП). С точки зрения электричества коаксиальный кабель замыкает контур между источником и приемником, где центральная жила кабеля является сигнальным проводом, а экран – заземляющим. Поэтому передачу по коаксиальному кабелю и называют несимметричной передачей.

В охранном телевидении чаще всего используется коаксиальный кабель RG-59/U, который может успешно и без корректоров передавать ч/б сигналы на расстояние до 300 м и цветные – на расстояние до 200 м.

Еще один популярный кабель – это RG-11/U, более толстый и дорогой. Максимальная рекомендованная длина для него – до 600 м для ч/б сигнала и 400 м для цветного сигнала. Существуют также более тонкие коаксиальные кабели с импедансом 75 Ом и диаметром всего 2,5 мм и даже плоские коаксиальные кабели. Они очень удобны для перегруженных участков передачи множества видеосигналов, например, многовходовых матричных коммутаторов. Максимальная длина такого кабеля намного меньше, чем у толстых кабелей, но ее вполне достаточно для соединений и перемычек.

4.8.2. Передача видеосигнала по витой паре

Витая пара — альтернатива коаксиальному кабелю. Этим кабелем пользуются в ситуациях, когда необходимо проложить линию длиной больше двухсот метров. Это особенно выгодно, когда пара проводов уже протянута между двумя точками.

Если используются обычные провода, то кабель витой пары обходится довольно дешево, но если используется особый кабель (рекомендованный производителями), с минимум 10-20 скрутками на один метр и защитной оболочкой, то это будет гораздо дороже.

Передачу видеосигнала при помощи витой пары также называют симметричной видеопередачей. Ее идея очень проста и отличается от несимметричной (коаксиальной) передачи видеосигнала. А именно: чтобы минимизи-

ровать внешние электромагнитные помехи, по витой паре передается сбалансированный сигнал. Все нежелательные электромагнитные помехи и шум в конечном счете одинаково воздействуют на оба провода. Вот почему лучше использовать специальные кабели, в которых оба провода одинаково подвержены наводкам и имеют одинаковое падение напряжения. Когда сигнал достигает приемного конца линии на основе витой пары, он попадает на вход дифференциального усилителя с хорошо сбалансированным фактором коэффициента ослабления синфазного сигнала (КОСС). Этот дифференциальный усилитель считывает дифференциальный сигнал между двумя проводами.

Если два провода имеют схожие характеристики и достаточно закруток на метр (чем больше, тем лучше), на них будут одинаково воздействовать шумы, падение напряжения и наводки. Усилитель с хорошим КОСС на приемном конце линии устранит большую часть нежелательных шумов.

4.8.3. Радиочастотная беспроводная (эфирная) передача видеосигнала

Радиочастотная (РЧ) передача видеосигнала по модуляции напоминает микроволновую передачу. Однако основные различия заключаются в том, что частота модуляции лежит в ОВЧ и УВЧ (VHF и UHF) диапазонах и осуществляется «всенаправленная» передача сигнала. Направленная (директорная) антенна типа «волновой канал» (подобно внутренним антеннам, используемым для приема определенного телеканала) позволяет получать сигнал в более удаленных точках. Следует отметить, тем не менее, что в зависимости от норм, принятых в стране, мощность излучения не должна превышать определенный предел, а в случае такого превышения потребуется одобрение соответствующего органа, регулирующего использование частот.

Существенным недостатком использования радиочастоты в охранном телевидении является то, что сигнал может быть получен любым ТВ-приемником, находящимся на незначительном расстоянии. Правда, иногда это и требуется. Например, для работы системы в больших комплексах, где видеокамеры, наблюдающие за главным входом, подсоединены через коллективную антенну, так что арендаторы могут просматривать видеокамеру на определенном канале своих ТВ-приемников.

Радиочастотная связь не требует прямой видимости, поскольку РЧ-излучение (в зависимости от того, УВЧ это или ОВЧ) может проходить через кирпичные стены, дерево и другие неметаллические объекты. Расстояние распространения радиосигнала зависит от многих факторов, и лучше всего проверять это в конкретных условиях (там, где будет использоваться РЧ-передатчик).

4.8.4. Сотовая сеть

Передача изображения по мобильным телефонам — возможность привлекательная, особенно на фоне доступных сегодня технологий. Мобильный телефон с модемом в комбинации с ноутбуком легко можно дополнить про-

граммными и техническими средствами, необходимыми для обеспечения беспроводной связи и передачи изображений.

Здесь применимы все те же обсуждавшиеся выше принципы и концепции, за исключением скорости передачи, которая в этой сети ниже.

Цифровая сеть дает хорошую помехозащищенность, хотя ее охват в настоящее время не столь широк, как аналоговый мобильный сервис. Цифровая мобильная сеть быстро растет, и роуминг доступен в большинстве промышленно развитых стран. Это значит, что пользователи, находясь за границей, могут направлять вызов в цифровую сеть страны пребывания и делать звонки, не выходя на оператора. Понятно, для активации роуминга пользователь должен сообщить об этом поставщику услуг.

В цифровой сотовой сети возможно получить скорость в 9600 бит/с при использовании модемного режима. Существуют усовершенствованные GSM-технологии, делающие возможным повышение скорости передачи данных от 9,6 кбит до 14,4 кбит по одному каналу. Мультиплексируя до четырех каналов в один временной интервал оператор сможет предложить до 57,6 кбит, что в шесть раз выше доступных сегодня скоростей, а технологии сжатия позволят еще более увеличить скорость передачи.

4.8.5. Волоконная оптика

Волоконно-оптический кабель, если он корректно протянут и заделан – это лучшее и самое надежное средство передачи сигнала. Несмотря на то, что более тридцати лет этот тип кабелей использовался в удаленных телекоммуникационных линиях связи, даже в трансокеанских, в охранном телевидении избегали или отказывались от его использования.

Главной причиной стал страх перед неизвестной технологией, которая считалась «нежной и чувствительной», и к тому же «слишком дорогой».

Волоконно-оптический кабель имеет огромные преимущества перед другими средствами передачи сигнала, и хотя он считается дорогим и сложным при заделке, но со временем становится все дешевле и проще в использовании.

Самые главные преимущества – это иммунитет к электромагнитным помехам более безопасная передача, более широкая полоса пропускания и намного большая протяженность линии без усиления.

Волоконная оптика — это технология, в которой в качестве носителя информации используется свет; при этом не важно, о каком типе информации идет речь — аналоговом или цифровом. Обычно используется инфракрасный свет, а средой передачи служит стекловолокно.

Передача сигналов по стекловолокну имеет ряд преимуществ перед существующими «металлическими» средствами передачи. Это:

- очень широкая полоса пропускания.
- очень низкое ослабление сигнала, порядка 1.5 дБ/км по сравнению с 30 дБ/км для коаксиального кабеля RG-59 (для сигнала 10 МГц).

- волокно (являющееся диэлектриком) создает электрическую (гальваническую) изоляцию между передающим и принимающим концом линии, поэтому невозможно возникновение «земляных петель».
- свет как носитель сигнала полностью остается внутри волоконно-оптического кабеля, поэтому не вызывает помех в соседних кабелях или других волоконно-оптических кабелях.
- стекловолокно не чувствительно к внешним сигналам и электромагнитным помехам (ЭМП), поэтому совершенно не важно, рядом с каким блоком питания будет проходить кабель — 110 В, 240 В, 10 000 В переменного тока или совсем близко от мегаваттного передатчика. Даже если молния ударит в одном сантиметре от кабеля — никаких наводок не будет.
- волоконно-оптический кабель миниатюрен и легок.
- невозможно сделать ответвление волоконно-оптического кабеля, не повредив при этом качества сигнала, что немедленно обнаруживается на принимающем конце линии. Это особенно важно для систем безопасности.
- цена волоконно-оптического кабеля падает с каждым днем. Обычный волоконно-оптический кабель стоит от $1 до $5 метр в зависимости от типа.

Волоконно-оптический кабель имеет больше преимуществ, чем какой-либо другой. Многие годы волоконно-оптический кабель использовался в телекоммуникациях и теперь становится все более популярен в охранном телевидении и системах безопасности.

По мере усовершенствования технологии концевой заделки и сращивания кабеля, а также его удешевления, все больше систем охранного телевидения и безопасности будут использовать волоконную оптику.

Волоконно-оптические устройства миниатюрны. Внешний диаметр используемого в охранном телевидении и системах безопасности кабеля составляет всего лишь 125 мкм. Стекловолокно – материал относительно прочный, но все же легко ломается, если его изогнуть на угол меньший определенного минимального радиуса. Поэтому характеристики кабеля должны обеспечивать адекватную механическую защиту и ударопрочность, сохраняя минимальный угол изгиба и обеспечивая легкость при укладке и обслуживании кабеля и стабильное качество передачи в течение времени жизни системы.

По конструкции волоконно-оптические кабели могут различаться довольно значительно: простой одноволоконный кабель, вставленный в трубку, стержень с пазами (открытый канал), ленточный, с защитным материалом (не обладающим оптическими свойствами).

4.9. Дополнительное оборудование в системах охранного телевидения

Многие компоненты систем охранного телевидения можно отнести к дополнительным. Некоторые из них понятны и просты в использовании, дру-

гие более сложны. Начнем с очень простого механизма – поворотного устройства.

При заказе или проектировании системы охранного телевидения сразу возникает вопрос сколько видеокамер будет входить в систему и какого типа – установленные фиксированно или на поворотном устройстве.

Фиксированные видеокамеры устанавливаются на кронштейне, при этом используются объективы с фиксированным фокусным расстоянием, а видеокамера «смотрит» только в одном направлении, не изменяя своего положения

Альтернативой фиксированным видеокамерам являются видеокамеры, положение которых в пространстве можно изменять (с помощью поворотного устройства). Такая видеокамера помещается на способную поворачиваться платформу, при этом обычно используются вариообъективы с сервоуправлением, так что весь комплекс может поворачиваться в горизонтальной и вертикальной плоскостях, увеличивать изображение объектов и осуществлять фокусировку.

В терминологии охранного телевидения видеокамеры этого типа называются «PTZ-камерами» и далее будет использован именно этот термин для обозначения видеокамеры, которая, кроме функций поворота, наклона и увеличения, обладает функциями фокусировки и дистанционного управления диафрагмой.

Типичное поворотное устройство имеет боковую платформу, на которую устанавливается нагрузка (видеокамера с вариообъективом в термокожухе). Существуют поворотные устройства с верхним расположением платформы, они отличаются по величине номинальной нагрузки, которая зависит от центра тяжести нагрузки. В случае поворотных устройств с боковыми платформами центр тяжести располагается ниже, это означает, что из двух типов устройств (при одинаковых электродвигателях и вращающем моменте) боковая платформа имеет большую номинальную нагрузку. Из этого не стоит делать выводов о том, что поворотные устройства с платформой сверху хуже, разница касается только номинальной нагрузки, которая в последние годы не является столь критичной, так как размеры видеокамер, объективов и, соответственно, кожухов, становятся меньше.

Имеется и другое направление в области поворотных устройств, которые по их внешнему сходству с куполами называют как купольные поворотные устройства. Логичнее подобные функционально и конструктивно законченные приборы называть как скоростные поворотные видеокамеры Едва ли не главная черта этих устройств, в отличие от традиционных поворотных устройств, достаточно инерционных – это высокая скорость поворота, что обеспечивается за счет малой массы собственно видеокамеры.

Они работают так же, как и обычные поворотные устройства, но внутри куполов находятся и механизм поворотного устройства, и управляющая электроника. Заключенные в прозрачные или полупрозрачные сферы или полусферы, такие устройства выглядят вполне приемлемо даже в интерьерах, требующих эстетического подхода. В связи с миниатюризацией видеокамер и объективов поворотные купола тоже становятся меньше в диаметре. Сегодня большинство устройств имеет всего 300-400 мм в диаметре.

Одна из главных проблем скоростных поворотных видеокамер – это оптическая точность. Очень трудно полностью избавиться от искажений, особенно если прозрачная полусфера изготавливается стеклодувным методом. Лучшая точность достигается при использовании литых куполов, но они дороже. Более толстые полусферы вызывают больше искажений, особенно когда объектив увеличивает изображение. Так что наилучшее оптическое качество имеют тонкие и литые полусферы.

Кожухи используются для защиты видеокамер от воздействия внешней среды и/или для маскировки направления видеонаблюдения.

Кожухи могут быть простыми в конструкции, установке и использовании, но они в равной мере могут влиять на качество изображения и срок службы видеокамеры, если не защищают ее должным образом от дождя, снега, пыли и ветра, или если они низкого качества.

Кожухи бывают самых разных размеров и форм, в зависимости от применения видеокамеры и ее длины. Раньше видеокамеры с передающими трубками и вариообъективами были намного больше, и для них требовались кожухи длиной в 1 метр и массой более 10 кг. Сегодня ПЗС-видеокамеры становятся все меньше, то же справедливо и в отношении объективов, и поэтому кожухи тоже становятся меньше.

В последние годы много внимания уделялось эстетике и функциональности кожухов, в частности, простоте доступа для обслуживания, скрытию кабельной подводки и подобным вопросам.

В наши дни, с уменьшением размеров видеокамер, вместо традиционных кожухов часто используются тонированные купольные системы, которые гораздо лучше вписываются в интерьер помещений и прекрасно сочетаются с архитектурой зданий.

Часто считается, что стекло кожуха не имеет большого значения, но если стекло неподходящего качества, то оптические искажения и спектральные ослабления могут повлиять на качество изображения. Другой важный фактор — это прочность стекла, необходимая для защиты видеокамеры в требующей этого обстановке. Оптическая точность и однородность еще более критичны для купольных видеокамер, так как в этом случае более заметно влияние оптической точности и искажения стекла (пластика) на качество изображения. Тонированные купола часто используются для маскирования направления визирования видеокамеры. В случае тонированных куполов следует учитывать ослабление света.

Многие кожухи имеют встроенный подогрев и вентилятор. Подогрев может понадобиться в районах с большой влажностью, где ожидается много льда и снега.

В районах с высокими температурами следует использовать вентиляторы, иногда их можно комбинировать с подогревателями. Источник электропитания для вентилятора может быть либо переменного, либо постоянного тока; следует выбирать вентиляторы хорошего качества, так как вентиляторы постоянного тока рано или поздно приведут к возникновению искр от вращения щеток, наводящих помехи на видеосигнал.

5. ВЫБОР ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ

Особое значение имеет правильное применение технических средств защиты, их тактически верное расположение в зонах безопасности и согласованность в работе.

При выборе средств защиты необходимо обратить внимание на:

- совместимость;
- условия эксплуатации;
- помехоустойчивость;
- электропитание;
- срок службы;
- функции управления..

При формировании требований к системе безопасности для защиты средних и крупных объектов целесообразно использовать следующие средства защиты.

1. Для периметра территории объекта:

- различные ограждения и заборы;
- препятствия, которые должны затруднить передвижения нарушителя по территории объекта и повысить вероятность его обнаружения системой сигнализации;
- специально оборудованные въезды и проходы на территорию, где находятся первые посты охраны, контролирующие доступ посетителей и проезды автомашин к зданиям. В последнее время получили распространение быстро выдвигающиеся (по сигналу тревоги) из полотна въездной дороги железобетонные препятствия-пандусы;
- систему охранной сигнализации для защиты всего периметра объекта или особо уязвимых его частей;
- систему охранного телевидения для визуального наблюдения за периметром территории объекта, за проходами и въездами на территорию, а также за наиболее важными участками территории, такими как склады, стоянки автомашин и т. д.;
- система дежурного и тревожного освещения территории объекта: дежурное освещение включается постоянно в ночное время, а тревожное освещение только после срабатывания сигнализации, для освещения наиболее важных зон территории и подходов к зданиям.

2. Для периметра здания:

- средства инженерной защиты первого этажа здания, такие как решетки, ставни на окна, на кондиционеры, усиленные рамы из металлических конструкций с усиленными анкерами, усиленные (металлические с внутренними запорами) запасные и пожарные двери;
- систему охранной сигнализации периметра первого этажа;
- систему охранного телевидения для визуального наблюдения за периметром здания и подступами к его основным и запасным входам;

– систему охранного освещения периметра здания и подступов к основным и запасным входам;

– специально оборудованный элементами инженерной защиты безопасный вход в здание, который может в рабочее время быть открытым для посетителей или иметь дистанционно управляемые замки, а в нерабочее время закрываться на внутренние запоры и усиливаться дополнительными решетками, сетками или ставнями.

3. Для представительской зоны здания (зал посетителей и клиентов):

– систему охранного телевидения для наблюдения за обстановкой в зале для посетителей и за основным входом;

– систему конспиративного охранного телевидения для постоянного наблюдения и непрерывной 24-часовой видеосъемки особо важных зон зала посетителей (подходов к кассам и проходу в служебные помещения здания);

– систему тревожного оповещения (звонки, сирены), которая включается службой безопасности или персоналом объекта при возникновении угрозы;

– систему охранного освещения наиболее важных зон (в ночное время);

– систему радиосвязи или сигнальной связи для сотрудников службы безопасности, которые могут дежурить в зале, как в форме, так и конспиративно, не привлекая внимания посетителей.

4. Для административно-хозяйственной зоны:

– систему охранной сигнализации таких важных помещений, как склады и хранилища в подвале и на первом этаже здания;

– средства инженерной защиты складских и подвальных помещений (усиленные двери, ставни на окна и вентиляционные решетки, усиленные засовы);

– систему охранного телевидения для визуального наблюдения за складскими помещениями, которая включается периодически или от системы охранной сигнализации.

5. Для зоны служебных и особо важных помещений:

– систему охранной сигнализации некоторых служебных и всех особо важных помещений – кабинетов руководителей объекта и комнаты для переговоров;

– систему защиты от подслушивания в кабинетах руководителей объекта и в комнате для переговоров;

– систему охранного телевидения для наблюдения проходов в служебные помещения;

– центральный пост службы безопасности, где осуществляется круглосуточный контроль всех систем защиты объекта, пост имеет дополнительную инженерную защиту, такую как усиленные стены, двери и замки, пуленепробиваемое стекло.

6. *Для зоны сейфовых помещений и банка данных:*

– тамбурный (двухдверный) проход мимо поста охраны, который управляет работой тамбура;

– инженерную защиту сейфовых помещений, такую как усиленные стены, пол и потолок, сейфовая дверь с сейфовым замком, усиленные вентиляционные решетки (помещение должно быть без окон);

– систему охранной и тревожной сигнализации на открывание двери сейфовых помещений и всех сейфов;

– систему скрытого охранного телевидения для круглосуточного наблюдения и видеосъемки действий на посту охраны и подходов к сейфовому помещению;

– систему защиты от снятия информации из банка данных и его коммуникаций;

– систему охранной сигнализации для защиты аппаратуры банка данных и хранилища носителей информации.

Дополнительно в зданиях объекта, во всех его зонах, должны быть оборудованы системы пожарной сигнализации и тушения пожара.

ЛИТЕРАТУРА

1. Краснюк Д. В., Хованский В. А. Инженерно-техническая безопасность: Учебно-практическое пособие / Московский государственный университет экономики, статистики и информатики. – М.: МЭСИ, 1999. – 88 с.

2. Петраков А. В., Лагутин В.С. «Телеохрана», Москва, Энергоатомиздат, 1998 г.

3. Абрамов А.М., Никулин О.Ю., Петрушин А.Н. «Системы управления доступом», Москва, «ОБЕРЕГ-РБ», 1998 г.

4. Владо Демьяновски «CCTV. Библия охранного телевидения» / пер. с англ. – М.: ООО «Ай-Эс-Пресс», 2003 г. – 344 с.

5. Магауенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие. – М.: Горячая линия – Телеком, 2004. – 367 с.

6. Магауенов Р. Г. Охранная сигнализация и другие элементы систем физической защиты. Краткий толковый словарь. – М.: Горячая линия – Телеком, 2007. – 97 с.

7. РД-78.147-93 «Единые требования по технической укрепленности и оборудованию сигнализацией охраняемых объектов».

8. РД-78.143-92 «Системы и комплексы охранной сигнализации, элементы технической укрепленности объектов. Нормы проектирования».

9. РД-78.145-93 «Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ».