**Аннотация**

В дипломной работе рассматривается интегрированные системы безопасности (ИСБ), ее состав, функции, применение в авиапредприятии. Напрямую задействовать и использовать ИСБ можно в службе авиационной безопасности (САБ). ИСБ позволяет контролировать все действия, происходящие на территории аэропорта. Такие как:

* контроль управление доступом;
* обеспечение пожарной безопасности;
* телевизионное наблюдение.

Использование ИСБ ведет к централизированному контролю над обеспечением авиационной безопасности

Количество страниц – 73, таблиц – 2, рисунков – 1

**Условные сокращения**

ИСБ – интегрированная система безопасности;

САБ – служба авиационной безопасности;

ТВН – телевизионное наблюдение;

ВС – воздушное судно;

ГА - гражданская авиация;

АБ – авиационная безопасность;

ВТ – воздушный транспорт;

НКС – наставление кризисных ситуаций;

АНВ – акты незаконного вмешательства;

ЭМС – электромагнитная совместимость;

ТСО – технические системы охраны;

ЭМП – электромагнитные помехи;

ИСО – интегрированные системы охраны;

КСБ – комплексные системы безопасности;

ТСОПС – технические системы охранно-пожарной сигнализации;

ПО – программное обеспечение;

ИТСБ – интегрированные технические системы безопасности;

СБ – служба безопасности;

ПК – программный комплекс;

ППКОП – прибор приемно-контрольный охранно-пожарный;

э. д. с. – электродвижущая сила;

ИК – инфракрасный;

СВЧ – сверх высокие частоты;

НИЦ – научно-исследовательский центр;

МВД – министерство внутренних дел;

СО – система охраны;

ОПС – охранно-пожарная сигнализация;

СИД – светодиодные индикаторы.

**Оглавление**

Введение

Глава 1. Авиационная безопасность авиапредприятия

1.1 Акты незаконного вмешательства

1.1.1 Терроризм на воздушном транспорте

1.1.2 Защита ГА от АНВ

1.2 Служба авиационной безопасности

1.3 Классификация технических средств и системы обеспечения безопасности авиапредприятия

Глава 2. Интегрированные системы безопасности (ИСБ)

2.1 Составные части ИСБ

2.1.1 Функционирование системы ИСБ

2.1.2 Интеграция техники систем безопасности

2.1.3 Уровни интегрирования

2.1.4 Преимущества ИСБ

2.2 Интеграция средств систем охраны

2.2.1 Управление ИСБ

2.3 ИСБ OnGuard 2000 с открытой архитектурой

2.3.1 Открытая архитектура

2.3.2 ИСБ OnGuard 2000

2.3.3 Неограниченная емкость системы

2.3.4 Другие возможности OnGuard 2000

2.4 ИСБ ППКОП «Сфера 2001»

2.4.1 Основные возможности прибора

2.4.2 Состав системы

Глава 3. Элементы ИСБ

3.1 Электрические измерения неэлектрических величин

3.1.1 Реостатные датчики

3.1.2 Проволочные датчики

3.1.3 Датчики контактного сопротивления

3.1.4 Индуктивные датчики

3.1.5 Емкостные датчики

3.1.6 Магнитоупругие датчики

3.2 Индукционные, термоэлектрические и пьезоэлектрические датчики

3.2.1 Индукционные датчики

3.2.2 Термоэлектрические датчики

3.2.3 Обращенные датчики

3.3 Усиление сигналов датчика

3.4 ИК-пассивные датчики

3.4.1 Установка и использование ИК-датчиков

3.5 Магнитоконтактные и электроконтактные датчики

3.6 Радиоволновые и комбинированные детекторы движения

3.7 Системы ограждений и охранные извещатели

3.7.1 Понятие извещателя

3.7.2 Выбор типа извещателя

3.7.3 Классификация извещателей

3.7.4 Принцип работы извещателей

3.8 Аналоговые извещатели и их свойства

Выводы и рекомендации

Список используемой литературы

**Введение**

Гражданская авиация - одна из транспортных структур наиболее подверженная чрезвычайным происшествиям, таким как пожары, акты незаконного вмешательства и другие негативы пагубно влияющие на работу данной отрасли в целом. Как следствие, гражданская авиация вынуждена оснащать свою территорию, здания и помещения, а также технический и обслуживающий персонал по последнему слову современной техники.

В России на рынке технологий представлено немалое количество систем безопасности как отечественного производства, так и зарубежного.

Структура авиапредприятия состоит из служб, которые напрямую или косвенно работают для обеспечения безопасности полетов.

Но есть служба авиационной безопасности (САБ), которая напрямую занимается вопросом по осуществлению безопасности в авиации. Спектр применяемых систем и средств различен. Но эти системы работают не в комплексе с другими, а лишь опосредственно.

В дипломной работе рассматриваются **интегрированные системы** **безопасности (ИСБ)**, их назначения, состав, какие функции они выполняют.

Это набор технических средств, включающих охрану и тревожную сигнализацию, средства обнаружения возгораний, оповещения о них, средств пожаротушения, системы ТВ – наблюдения и контроля доступа, объединенных с помощью компьютера систему и обработки информации, посредством программного продукта, реализующего все организационные, технические и эксплуатационные критерии, объединения систем безопасности, т. е. «интеграция» позволяет:

* минимизировать капитальные затраты на оснащение объекта, аппаратная часть значительно уменьшается как за счет полного исключения дублирующей аппаратуры в разных системах, так и за счет увеличения эффективности работы каждой системы;
* уменьшать время поступления более полной и объективной информации о состоянии объекта, необходимой оператору в экстремальной ситуации для принятия правильного решения. Кроме того, оптимизировать штат охраны, что существенно снижает расходы на содержание, оснащение и лицензирование охранников;
* повышать защищенность самой системы от внешнего воздействия, от несанкционированного доступа к аппаратуре и базам данных, что в результате должно исключать влияние субъективного фактора;
* разграничивать права и приоритеты в доступе к хранению и использованию полученной информации;
* создавать с помощью необходимого комплекса аппаратно-технических средств гибкие логические структуры в интеграции средств безопасности, по принципу «есть задача – всегда есть решение».

ИСБ изначально состоит из элементов, которые отвечают а прием и обработку той информации, которая после преобразований будет сигнализировать:

* о проникновении на территорию аэропорта;
* о пожарной сигнализации;
* задымлении помещений;
* местонахождении персонала.

И этими элементами являются электрические измерения неэлектрических величин, т. е. разнообразные типы датчиков, извещателей и сигнализаторов.

**Глава 1. Авиационная безопасность авиапредприятия**

Обеспечение авиационной безопасности является одной из важнейших задач гражданской авиации. Ей уделяется все возрастающее внимание в связи с обострением терроризма, политическим и экономическим шпионажем, национализмом, разжиганием идеологических и религиозных противоречий.

Объектами нападений террористических групп, в зависимости от поставленных ими целей, являются различные учреждения, офисы фирм, посольства, транспортные средства: автобусы, морские и воздушные суда. Последние подвергаются захвату наиболее часто.

Этому служат следующие предпосылки:

* реальность захвата и угона воздушного судна (ВС) за границу представляет минимальную опасность для преступников и большую угрозу жизни пассажиров и экипажа;
* захват и угон ВС расценивается преступником как одно из результативных средств достижения задуманной им цели;
* выполнить преступные действия террорист способен при использовании минимальных сил и средств. Обычно одно лицо (как подтверждает статистика) осуществляет похищение ВС. Преступление совершается индивидуально, независимо от того, является ли его исполнитель одиночкой или соучастником преступной группы;
* ВС представляет значительную ценность, легко поступиться которой государство не может;
* действующие группировки преступников считают захват ВС наиболее легким и дешевым способом приобретения популярности, освобождения отбывающих наказание террористов, получения выкупа. Немаловажное значение для них имеет побег в государства, предоставляющие им убежище;
* в случае катастрофы большинство пассажиров погибает, террорист остается анонимным лицом.

Бомбы, гранаты, пистолеты стали средством и оружием принуждения, применяемыми террористами. Они отдают себе отчет в собственной силе. Ничто не служит демонстрацией решительности лучше, чем взрывной заряд в руках безрассудного преступника.

ГА уязвима для нападения в любом месте и в любое время, так как:

* сам характер авиационной отрасли позволяет преступнику приступить к теракту, не находясь в непосредственной близости от намеченного объекта;
* действующие в настоящее время группы террористов организованы и располагают значительными современными средствами для нападения на ВС.

Нападение на ВС ГА, а также другие транспортные средства, их захват, угон и уничтожение остается на сегодняшний день одной из самых распространенных и опасных форм терроризма. ГА стала подвергаться более зловещим, с летальным исходом, методам нападения террористов.

Угроза АБ носит динамический характер и представляет собой ряд различных ступеней интенсивности, требующих применения соответствующего набора мер по степени возрастания их сложности.

Слабая организация работы по обеспечению АБ, оснащенность техническими средствами (досмотра, охраны) и недостаточная квалификация персонала службы АБ в целом создает условия для проведения террористических актов на ВТ.

**1.1 Акты незаконного вмешательства**

К авиационной безопасности относится комплекс мер, а также людские и материальные ресурсы, предназначенные для защиты гражданской авиации от актов незаконного вмешательства.

Под актом незаконного вмешательства понимают:

1. Насилие в отношении лица, находящегося на борту воздушного судна в полете и угрожающего безопасности этого воздушного судна;
2. Разрушение воздушного судна, находящегося в эксплуатации, или причинение этому воздушному судну повреждения, которое выводит его из строя или угрожает его безопасности;
3. Помещение или совершение действий, приводящих к помещению на воздушное судно, находящееся в эксплуатации, каким бы то ни было способом устройства или вещества, которое может разрушить воздушное судно или причинить ему повреждения, несущие угрозу безопасности в полете;
4. Разрушение или повреждение аэронавигационного оборудования или вмешательство в его эксплуатацию, если такой акт может угрожать безопасности воздушных судов в полете;
5. Сообщение заведомо ложных сведений, создающих угрозу безопасности воздушного судна в полете;
6. Незаконное и преднамеренное использование любого устройства, вещества или оружия для совершения акта насилия в отношении лица в аэропорту, обслуживающего международную гражданскую авиацию, который причиняет или может причинить вред здоровью или смерть;
7. Разрушение или серьезное повреждение оборудования и сооружений авиапредприятия, либо расположенных в аэропорту воздушных судов, не находящихся в эксплуатации, либо для нарушения работы служб авиапредприятий, если любой акт угрожает или может угрожать безопасности в этом авиапредприятии.

Диверсия - акт или преднамеренное упущение, имеющее целью вызвать злоумышленное или бессмысленное уничтожение имущества, ставящее под угрозу деятельность авиапредприятия и ее спецслужб или приводящие к незаконному вмешательству в эту деятельность.

Досмотр - применение технических или других средств, предназначенных для обнаружения оружия, взрывчатых веществ или других опасных устройств, которые могут быть использованы для совершения акта незаконного вмешательства.

Контроль в целях безопасности - меры, с помощью которых может быть предотвращен пронос оружия, взрывчатых веществ или предметов, которые могут быть использованы в целях совершения актов незаконного вмешательства.

Оборудование для обеспечения безопасности - специальные устройства, предназначенные для использования самостоятельно или как часть, какой либо системы при обеспечении защиты от актов незаконного вмешательства в деятельность авиапредприятия.

Охраняемая зона ограниченного доступа - те зоны авиапредприятия, здания или средства, доступ в которые ограничен или контролируется в целях обеспечения авиационной безопасности.

Программа безопасности - меры, введенные для защиты гражданской авиации от актов незаконного вмешательства.

* + 1. **Терроризм на воздушном транспорте**

В последние годы в нашей стране резко возросли случаи терроризма. В современных условиях - условиях быстрого прогресса видов оружия и, прежде всего, оружия массового поражения, терроризм стал явлением исключительно опасным. Основу современного терроризма образуют социальная неустойчивость в мире, национальные конфликты и, связанные с ними, крайний национализм, экономическая отсталость и религиозный фанатизм. В масштабах одного государства правовые и организационные методы борьбы с терроризмом подразумевают совместные действия всех государственных правоохранительных органов по опережающему выявлению террористических угроз, пресечение попыток терроризма и его осуждение.

Акты терроризма особенно ярко проявляются в гражданской авиации. Кроме захвата и угона воздушных судов (ВС) имеют место угрозы в адрес воздушного транспорта, несанкционированные проникновения в ВС, нападение на земле с захватом заложников с целью шантажа и вымогательства, с требованием предоставления воздушного транспорта для выезда из страны.

Преступные акты воздействия на ГА приобретают постоянный характер, начиная с 1984г. Количество угроз в адрес ГА постоянно возрастает. В период с 1990г. по 1994г. количество актов незаконного вмешательства в деятельность воздушного транспорта по сравнению с 32 предшествующими годами удваивается. За недавние годы (с 1990г. по 1995г.) произошло 62 случая попыток захвата и угона ВС, что составляет примерно 33% от зафиксированных аналогичных случаев в мире. Разнообразие целей, мотивов и личностей самих террористов, а также возможностей проведения теракта придает ему свойства как закономерного, так и случайного события. Случайным является только место, время и вид акта незаконного вмешательства.

В каждом авиапредприятии составляется программа обеспечения авиационной безопасности. Она включает в себя три состава действий:

* действия до кризисной ситуации;
* действия во время кризисной ситуации;
* действия после ликвидации кризисной ситуации.

Программа документально оформляется в виде Наставления. Наставление по планированию обеспечения безопасности ГА и действиям руководителя в кризисной ситуации, иначе называемое Наставлением для кризисных ситуаций (НКС), служит руководством для руководителей авиапредприятия при составлении собственных планов действий в кризисных ситуациях.

НКС - документ, в котором подробно рассматриваются различные аспекты действий руководства авиапредприятия в кризисной ситуации и при несчастных случаях.

Первым шагом в разработке системы управления в кризисных ситуациях для любой организации является оценка действительной или предполагаемой уязвимости этой организации. Второй шаг, который должен быть предпринят организацией в разработке системы руководства в кризисной ситуации - это выявление наличия ресурсов (как внутри, так и вне организации), на которые можно рассчитывать в кризисных ситуациях. К основным категориям ресурсов относятся: люди (специалисты и эксплуатационный персонал); средства обслуживания (эксплуатация, коммунальные услуги, безопасность людей, административно-хозяйственная служба); оборудование (специализированное оборудование, автомобили, подъемные краны, трапы и т. д.); средства связи (телефоны, радиостанции, факсы и т. д.); охрана - важнейший ресурс в разрешении кризисных ситуаций.

На завершающей стадии разработки системы руководства в кризисных ситуациях составляется структурная схема взаимодействия подразделений и должностных лиц с указанием каналов связи и располагаемых ресурсов. Обязанности должностных лиц по обеспечению авиационной безопасности отражаются в должностных инструкциях. Администрация авиапредприятий кроме того руководствуется Положением "О федеральной системе защиты деятельности ГА от актов незаконного вмешательства.

Беспрецедентный случай незаконного вмешательства в деятельность ГА произошедший 11 сентября 2001 года в США.

Одновременно (7:58…8:10 утра) были захвачены террористами-смертниками 4 пассажирских самолета. Первый - «Боинг 767» авиакомпании «Америкэн Эйрлайнз» вылетел из Бостона в Лос-Анджелес, однако, после захвата его террористами, самолет повернул на Нью-Йорк и врезался в северную башню Всемирного торгового центра. Погибло 92 человека, включая экипаж.

Второй - «Боинг 767» авиакомпании «Юнайтед Эйрлайнз» вылетел из Бостона через 13 минут е первого, и должен был лететь по тому же маршруту в Лос-Анджелес. Но. как и первый самолет, сменил маршрут и взял курс на Нью-Йорк Прошло всего 18 минут после того, как покачнулась от страшного удара и взрыва северная башня, и второй самолет врезался в южную башню Всемирного торгового центра. Погибло 65 человек, включая экипаж. Общее число погибших в результате тарана и разрушения зданий Всемирного торгового центра составило более 3 тысяч человек.

Третии - «Боинг 757» авиакомпании «Америкэн Эйрлайнз» вылетал из вашингтонского аэропорта Даллес в Лос-Анджелес Однако изменил курс и врезался в западное крыло министерства обороны США – Пентагон. На борту самолета находилось 64 человека.

Четвертый - «Боинг 757» авиакомпании «Юнайтед Эйрлайнз» вылетел из Нью-Йорка в Сан-Франциско. Через 2 часа 9 минут после вылета самолет рухнул в окрестностях Питсбурга. Погибло 45 человек, включая экипаж. Предполагалось, что объектом нападения захваченного самолета могла стать атомная электростанция.

* + 1. **Защита Гражданской Авиации от актов незаконного вмешательства**

Во всех вопросах, связанных с защитой гражданской авиации от актов незаконного вмешательства, первоочередной целью каждого государства является безопасность пассажиров, экипажа, наземного персонала и общественности в целом. Эффективное обеспечение безопасности гражданской авиации может быть достигнуто путем разработки, применения и поддержания всеобъемлющих, гибких и эффективных законов, правил, программ, мер и процедур.

В каждом аэропорту необходимо принять программу безопасности гражданской авиации. Ввиду различия эксплуатационных особенностей, экологических аспектов и характеристик уязвимости для каждого аэропорта необходимо разрабатывать индивидуальную программу безопасности.

Целью программы является обеспечение мер защиты по сохранению жизни и здоровья пассажиров, членов экипажей гражданских воздушных судов, обслуживающего персонала авиапредприятия, охраны воздушных судов и средств авиапредприятия, а также предупреждение и пресечение захвата и угона воздушного судна путем проведения комплекса мероприятий по выполнению норм, правил и процедур по авиационной безопасности, определенных "Положением о Федеральной системе обеспечения защиты деятельности гражданской авиации от актов незаконного вмешательства", утвержденным постановлением Правительства Российской Федерации от 30 июля 1994 г. № 897.

Назначение программы — разработка процедур и организационных мероприятий по обеспечению в авиапредприятии в процессе производственной деятельности мер авиационной безопасности для регулирования вопросов авиационной безопасности в базовом, а также во всех промежуточных аэропортах назначения, обслуживаемых авиапредприятием, где осуществляется посадка пассажиров и погрузка грузов, для авиатранспортировки или выполнения авиационных работ.

Выполнение требований программы обязательно для всех физических и юридических лиц, а также сотрудников авиакомпаний и сторонних организаций-заказчиков, в интересах которых выполняются авиационные работы и услуги.

Невыполнение или нарушение норм, правил и процедур по авиационной безопасности физическими и юридическими лицами влечет за собой уголовную или административную ответственность в соответствии с законодательством Российской Федерации.

Программа обеспечения авиационной безопасности может дополняться и изменяться в связи с принятием новых правовых актов, регламентирующих вопросы обеспечения авиационной безопасности эксплуатантов воздушного транспорта Российской Федерации.

* 1. **Служба авиационной безопасности**

САБ действует в соответствии со стандартами и рекомендациями ИКАО, положением о федеральной системе обеспечения защиты деятельности гражданской авиации от актов незаконного вмешательства, утвержденным постановлением правительства Российской Федерации от 30.07.94 г. № 897, приказами министра транспорта Российской федерации от 14.04.94 г. и от 17.10.94 г. № 76.

САБ осуществляет в аэропорту комплекс мероприятий по обеспечению безопасности ГА от АНВ в ее деятельность, а также усиливает (дополнительно) меры безопасности в период повышенной угрозы воздушному транспорту или чрезвычайных обстоятельств.

САБ взаимодействует с другими структурными подразделениями аэропорта, организациями и эксплуатантами воздушных судов, расположенными в аэропорту и пользующимися его услугами, а также территориальными органами ФСБ, МВД России и исполнительной власти при решении вопросов, отнесенных к ее компетенции.

Служба АБ разрабатывает программу АБ аэропорта и осуществляет ее реализацию, обеспечивает выполнение норм, правил и процедур по АБ и подчиняется непосредственно директору по АБ.

САБ в гражданской авиации имеет широкие полномочия по защите воздушного транспорта и его пассажиров от незаконного вмешательства в работу гражданской авиации и от уголовных актов насилия.

Первичным механизмом осуществления этих требований служит охрана аэропортов, представляющая собой самый важный ресурс компании эксплуатанта, предусмотренный в системе руководства в кризисно]! ситуации. Термин "охрана аэропорта" в данном случае означает людей, объекты и оборудование, используемые для обеспечения безопасности аэропорта и, в частности, в кризисной ситуации, либо в обычном j ом порядке, либо по устному или письменному соглашению. Это может включить в себя широкий спектр ресурсов обеспечения безопасности или ресурсов, имеющих к ним отношение, которыми располагает служба авиационной безопасности аэропорта и другие организации.

* 1. **Классификация технических средств и систем обеспечения безопасности авиапредприятия**

Создать систему безопасности — это значит, прежде всего, обосновать тактико-технические требования к ее материально-технической части.

Существующие инженерные и технические средства борьбы с терроризмом не универсальны. Они позволяют выявить и нейтрализовать террористические угрозы только при определенных условиях или сценариях развития событий. Очень часто при этом важны организация и технология защиты. Важную роль при этом играют временные требования по рациональной асинхронной противодействии угрозам. Изобразим графически динамику развития угроз и противодействий.

Можно считать процессы развития угрозы и противодействия процессами статическими во времени. В таком случае они описываются так называемыми вероятностными законами распределения. Если, в частности, обозначить (X\*) - закон для угрозы (т.е. вероятность ее реализации за время t), то функция 0 (1) будет возрастающей, стремящейся к 1. На рис.1 представлены расчетные данные относительной величины Т (1/ТР для различных значений Тх/Тр. Из них следует, что :

* чем больше время То - упреждения угроз и блокировки, тем больше эффективность защиты;
* при очень медленных реакциях системы на опасность (когда Тр\Тх) время упреждения или блокировки связано с эффективностью О следующим образом:

**Т > Т„ (1)**

Рассмотрим случай, когда среднее время реализации угрозы Тх = 10 минут, а среднее время прибытия сил быстрого реагирования Тр = 1 5 минут.

Здесь Т/Тр = 0,67. В отсутствии упреждения и блокировки эффективность защиты угроз получается невысокой, при То = 0, р = 40% . Однако при Т/Тр =4 , т.е. при наличии упреждения или блокировки угрозы со временем I ч. эффективность защиты возрастает до 99%.

На графике рис. 1. То - время упреждения и блокировки угрозы. Тр -время реакции системы на сигнал тревоги . За Тх - обозначим среднее время реализации угрозы.

Если считать, что все процессы случайные и подчиняются нормальному закону распределения, то для эффективности защиты, которую обозначим как Q справедливо соотношение:

**Q = 2 - еТо/Тр (1 + Тх./Тр) (1)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  | =0,99 |
|  |  |  |  |  |
|  |  |  |  | =0,95 |
|  |  |  |  | =0,90 |

0 0,50 1,0 1,5 2,0

Т Рис. 1

Можно сделать следующие выводы:

* + - * Наибольшие ассигнования на опережающие и блокирующие противодействия должны выделяться по тем направлениям, для которых эффективность защиты минимальна, а вероятность угроз ощутима.

Такими направлениями являются:

* + - * противодействие внешним угрозам (в форме силового проникновения);
      * противодействия внутренним угрозам (сговор, хищение собственности);
      * В первом случае основное внимание должно уделяться блокирующим мероприятиям с использованием инженерно-технических решений. Во втором упреждающим противодействиям, связанным с кадровой работой.

**Глава 2 Интегрированные системы безопасности (ИСБ)**

Обеспечение безопасности крупных объектов - крайне сложная задача. Ее решение требует учета множества взаимосвязанных факторов. Увеличение штата охранников и наращивание технических средств безопасности часто не дает желаемого результата: охранник не может контролировать все рубежи защиты. Поэтому вопрос повышения уровня безопасности решается нашей компанией иными средствами: с помощью построения интеллектуальных интегрированных систем (ИСБ).

ИСБ обладают высокой эффективностью и надежностью за счет взаимодополнения и резервирования технических средств. В ней отсутствуют избыточные линии связи, управление осуществляется оперативно и централизованно с помощью автоматизированных рабочих мест.

В последнее время наблюдаются тенденции к объединению технических средств обеспечения безопасности в единую интегрированную систему, включающую охранную сигнализацию, управление доступом, телевизионное наблюдение, контрольные и др. устройства. Интегральные системы бывают разного уровня, начиная от простого объединения в одну систему, например, охранной сигнализации и контроля доступом, до сложной системы управления.

**2.1 Составные части ИСБ**

Составными частями ИСБ являются:

* сеть датчиков, которая обеспечивает получение максимально полной информации со всего пространства, находящегося в поле зрения службы безопасности, позволяет воссоздать на центральном пункте наблюдения всестороннюю и объективную картину состояния помещений и территории объекта и работоспособности всей аппаратуры и оборудования;
* исполнительные устройства, способные при необходимости действовать автоматически или по команде оператора;
* пункты (или пункт) контроля и управления системой отображения информации, через которые операторы могут следить за работой всей системы в пределах своих полномочий;
* центральный процессор с программирующим устройством, наглядно представляющий информацию датчиков и накапливающий ее для последующей обработки;
* коммуникации, через посредство которых обеспечивается обмен информацией между элементами системы и ее операторами.

Такая структура интегрированной системы безопасности дает возможность обеспечить:

* контроль за большим количеством помещений с созданием нескольких рубежей защиты;
* иерархический доступ сотрудников и посетителей в помещения с четким разграничением полномочий по праву доступа в помещения и по времени суток и по дням недели;
* идентификация личности человека, пересекающего рубеж контроля доступа;
* слежение за точным исполнением персоналом охраны своих служебных обязанностей;
* предупреждение попадания на объект запрещенных материалов, веществ, оружия и устройств;
* взаимодействие постов охраны и органов правопорядка при несении охраны и в случае локализации происшествий;
* накопление документальных материалов для использования их при расследовании и анализе происшествий;
* оперативный инструктаж работников системы о порядке действий в различных штатных и нештатных ситуациях путем автоматического вывода на монитор текста инструкций в нужный момент.

Кроме того, гибкое программирование функций интегрированной системы дает возможность противодействовать таким ухищрениям для проникновения на защищенные объекты, как прерывание каналов передачи тревожной информации, нейтрализация части системы людьми, имеющими доступ к ее элементам, проникновение с сигналом тревоги и последующим уничтожением информации о происшествии, использование отклонений от предписанного порядка несения службы персоналом охраны, создание нештатных ситуаций в работе системы.

**2.1.1 Функционирование системы**

Ядро системы - центральный компьютер (сервер), который управляет подключенным к нему модулем охранно-пожарной сигнализации, цифрового видеонаблюдения и контроля доступа, а также модулями пожаротушения, оповещения, управления инженерными сетями здания и т.д. В ответ на событие, произошедшее в одной подсистеме, происходит соответствующее действие в Другой. Видеокамера показывает место, где сработал охранный датчик; контроллер системы доступа выключает свет и кондиционер в помещении, откуда ушел последний сотрудник, а затем ставит это помещение под охрану; на экране монитора происходит сравнение фотографии сотрудника и видеоизображения человека, предъявившего карту доступа.

Центральный компьютер собирает в единое целое данные от всех информационных систем и представляет ее операторам в доступном для восприятия графическом виде. Одновременно система осуществляет постоянный контроль за действиями охраны. В случае непреднамеренного или умышленного повреждения автоматизированных рабочих мест центральный сервер без потери контроля над системой зафиксирует все нештатные ситуации.

Большим преимуществом системы является возможность дистанционного сетевого управления, при котором все параметры модулей контролируются по цифровым сетям связи, будь то Ethernet (Internet), ISDN или просто телефонная линия. Наша система позволяет создавать точки мониторинга в различных местах организации, часто весьма удаленных друг от друга. Мощная защита предотвратит возможные попытки взлома или перехвата управления.

**2.1.2 Интеграция техники системы безопасности**

Программное обеспечение (ПО) компьютеров интегрированной технической системы безопасности (ИТСБ) должно централизованно и единообразно обслуживать подключенные к системе технические средства (видеокамеры, вообще система видеонаблюдения, система управления доступом, системы вентиляции и кондиционирования и что там еще потребуется). Но это не главное. Основное требование к интегрированной системе - обеспечение эффективного взаимодействия техники и людей (см. статью в предыдущем номере). ПО ИТСБ должно поддерживать отработку Службой Безопасности (СБ) различных алгоритмов реакции на плановые и, главное, внеплановые события. Существенно, что эти алгоритмы уникальны для каждого объекта. Поэтому важной чертой систем высокого класса (например, BSW у ЗАО "Компания Безопасность" и другие) является возможность не только настраивать автоматические реакции системы на события, но и задавать сложные алгоритмы с участием оператора (или даже нескольких операторов) системы, с участием линейных сотрудников СБ, с участием обычных сотрудников объекта (неспециалистов из СБ).

Различные человеко-машинные алгоритмы применяются уже давно, но сейчас по мере роста мощности и возможностей компьютеров широкого назначения, по мере накопления опыта применения таких систем, реализуются все более сложные внутри и все более простые снаружи (удобные для оператора) системы.

Минимальное требование, всегда предъявлявшееся к системе охранной сигнализации, - фиксация тревоги до ее подтверждения оператором. Сигнал тревоги (сирена) продолжается до тех пор, пока оператор не нажмет кнопку "сброса" тревоги. По мере совершенствования систем вместо нажатия на кнопку стал требоваться ввод кода, затем ввод индивидуального кода, с тем чтобы впоследствии можно было выяснить, кто именно проверил причину тревоги и отключил сирену.

Подобный алгоритм — верификация тревоги с ее последующим сбросом (если она ложная или несущественная) или, наоборот, с объявлением общей боевой тревоги и вызовом сил противодействия противнику (если тревога вызвана действительно серьезным посягательством). Пожалуй, это самый первый "человеко-машинный" алгоритм.

* + 1. **Уровни интегрирования**

Центральный процессор объединяет единую систему в группу:

* региональных подсистем (систему видео-наблюдения, контроля доступа, охранную и пожарные сигнализации, видео-базы данных пользователей и обеспечивает их взаимодействие, каждая из подсистем автоматически выполняет какие-либо действия при поступлении определенного сигнала от любой другой;
* местные контрольные устройства, являясь блоками, способными "принимать решения", управляют небольшой группой сигнализационных датчиков, считывателями карт, исполнительными устройствами (замками, шлагбаумами, лифтами и т. д.)
  + 1. **Преимущества интегрированных систем**

Интегрированные системы обладают следующими преимуществами:

1. Благодаря гибкой архитектуре, интегрированная система быстро конструируется из определенного набора модулей и блоков практически для любых условий и объектов разной величины;

2. В процессе эксплуатации легко наращивается нужное количество дополнительных объектов охраны, и совершенствуются функции системы путем подключения различных типов регистрирующих и исполнительных устройств (например, ведение электронной картотеки с изображениями пользователей системы, управления лифтами и дверьми, ведение отчетности о посещаемости и т.д.);

3. Возможна скрытая маркировка наиболее ценных предметов в помещении для того, чтобы регистрировался факт их выноса из данного помещения. При этом, если предмет выносит человек с «правами собственности», система лишь зафиксирует факт выноса (или приноса), в противном же случае подается сигнал тревоги;

4. При необходимости можно использовать контрольные панели со связью по радиоканалу для подключения к системе объектов, удаленных от центрального поста или в условиях целесообразности прокладки кабельной связи, Такие панели осуществляют связь по 100 из 160 возможным радиочастотам, причем конкретные радиочастоты определяются случайно, для каждого сеанса, что практически исключает возможность постороннего вмешательств в работу системы.

Система контроля доступа, например, рассчитана на любое количество дверей от одной до 4096. Охранные системы позволяют контролировать от 16 до 36000 сигнализационных точек. Системы видеонаблюдений могут иметь до 999 телекамер и 256 мониторов. Базы данных видео-идентификации способны обрабатывать неограниченное число изображений, при этом соблюдается полная интеграция систем в единую автоматизированную комплексную систему безопасности.

**2.2 Интеграция средств систем охраны**

Некоторые вопросы стандартизации требований по электромагнитной совместимости

В настоящее время оценка соответствия требованиям электромагнитной совместимости (ЭМС) является обязательной для всех радиоэлектронных устройств, изделий телемеханики, электро-, радиотехнического профиля и т.п. Технические средства и системы охраны, о которых пойдет речь в статье, относятся к таким изделиям

Оценка устойчивости технических средств и систем охраны (ТСО) к электромагнитным помехам (ЭМП) в общем случае может включать измерения таких параметров, как:

* уровень помех во внутренних цепях и соединениях узлов, блоков ТСО;
* режим работы отдельных узлов, блоков ТСО после воздействия установленного уровня помех;
* режим работы отдельных приборов, устройств, средств до, во время и после воздействия установленного уровня помех;
* функционирование интегрированных систем охраны и комплексных систем безопасности в целом: до, во время и после воздействия установленного уровня помех.

Испытания по первым трем видам могут проводиться в лабораторных условиях испытательных центров. Испытания по установлению работоспособности интегрированных систем охраны (ИСО), комплексных систем безопасности (КСБ) могут проводиться как в лабораторных условиях, так и на реальных объектах, что требует разработки специальных программ испытаний для каждой системы.

Требования к ЭМС технических средств и систем охраны в настоящее время устанавливаются по ГОСТ 30379-95 - ГОСТР 50009-92 "Совместимость технических средств охранной, пожарной и охранно-пожарной сигнализации электромагнитная. Требования, нормы и методы испытаний на помехоустойчивость и индустриальные радиопомехи".

В стандарте установлены регламентируемые характеристики устойчивости ТС ОПС к воздействию ЭМП по пяти степеням жесткости (первая - низшая). Выбор норм, методов испытаний и степеней жесткости осуществляют лица, разрабатывающие, согласовывающие и утверждающие техническое задание или технические условия на ТС ОПС в соответствии с ГОСТ 29280.

Отбор образцов для сертификационных испытаний проводят по ГОСТ 29037, обработку результатов измерений и их оценку по ГОСТ 16842, ГОСТ 29073 и ГОСТ 29280\*. В ранее разработанных стандартах подобные требования к ЭМС отсутствуют. Их нет среди основных параметров (ГОСТ 26342) и показателей (ГОСТ 4.188) ТСО.

В ГОСТ 27990-88"Средства охранной, пожарной и охранно-пожарной сигнализации. Общие технические требования" в качестве требований к перспективным ТС ОПС были введены следующие показатели:

* электрический импульс в цепи питания;
* электростатический разряд;
* кратковременное прерывание сети;
* электромагнитные поля.

В настоящее время срок действия стандарта фактически истек (до 01.01.2000 г.).

В ГОСТ Р 50775-95 (МЭК 839-1-88)Системы тревожной сигнализации Часть 1. Общие требования. Раздел 1. Общие положения" указано, что "системы охранной и охранно-пожарной сигнализации в части ЭМС должны соответствовать требованиям ГОСТ Р 50009, уровень допустимых радиопомех при работе систем тревожной сигнализации должен соответствовать ГОСТ 23511, а технических средств охранной и охранно-пожарной сигнализации - ГОСТ Р 50009". ' Требования по соответствию ГОСТ Р 50009 были введены при разработке группы стандартов на извещатели охранные, а также при формировании требований по ЭМС в ГОСТ Р 51241-98"Средства и системы контроля и управления доступом. Классификация. Общие технические требования и методы испытаний" и ГОСТ Р 51558-2000"Системы охранные телевизионные. Общие технические требования и методы испытаний". В этих стандартах для ГОСТ Р 50009 установлены следующие степени жесткости:

* 1-я или 2-я степени жесткости - нормальная устойчивость;
* 3-я степень жесткости - повышенная устойчивость;
* 4-я или 5-я степени жесткости - высокая устойчивость.

При изложении требований по ЭМС в стандартах имеется некоторое несоответствие, что можно в какой-то мере объяснить редкой

**2.2.1 Управление интегрированными системами безопасности**

Программный комплекс (ПК) APACS, разработанный российской компанией "ААМ Системз", является интеллектуальной основой интегрированной системы безопасности (ИСБ), строящейся на базе отечественного и зарубежного оборудования ведущих производителей. Его назначение – управление всей ИСБ в целом и каждой из подсистем в отдельности, организация эффективного взаимодействия между системой контроля управления доступом (СКУАХ охранно-пожарной сигнализацией (ОПС), системой теленаблюдения (CCVE), системами автоматики зданий и сооружений

Устойчивость и надежность обеспечиваются огромным практическим опытом, учитывающим особенности и потребности отечественного рынка - на территории России и стран СНГ ПК APACS внедрен более чем на 250 объектах. Каждая новая версия ПК APACS проходит тестирование в техническом отделе на устойчивость работы и совместимость с оборудованием.

Такое управление достигается за счет использования принципа интерактивности и наличия графического интерфейса с планами объекта в "дежурном режиме". Все события наглядно отображаются на мониторе. Кроме того, возможно прямое управление конкретным считывателем, охранным шлейфом, видеокамерой (и другими объектами системы) непосредственно с графических планов. Ценность оперативного работника в значительной степени зависит от скорости реакции, поэтому ПК APACS построен так, что охраннику, управляющему системой, достаточно просто "кликнуть мышью" по тревожному объекту для того, чтобы получить о нем более подробные сведения и управлять им напрямую. Например, оператор имеет возможность с помощью "мыши" открыть или заблокировать дверь, поставить или снять с охраны шлейф, просто указав данный объект на плане.

За счет автоматизации действий и реакций ПК APACS позволяет существенно снизить нагрузку на оператора, принимая на себя рутинную работу, и одновременно страхует его в экстремальных ситуациях. Становится возможным четкое выполнение однообразной, монотонной работы без срывов и ошибок, связанных с "притупившимся вниманием" охранника. Одновременно в экстренных ситуациях, когда зачастую необходима мгновенная реакция на внешние события, программа также не подведет. Следует отметить, что человек не исключается из процесса управления, просто он выполняет функции общего контроля и берет на себя управление в сложных нестандартных ситуациях (т.е. занимается тем, что у него лучше всего получается). Мощный программный «аппарат реакций» обеспечивает возможность программирования определенной последовательности действий системы в виде реакций на внешние сообщения. Это позволяет автоматически выполнять такие операции, как: постановка и снятие помещений с охраны, звуковое предупреждение оператора о событиях, вывод на монитор списка заранее подготовленных команд и пр.

Защита системы достигается за счет разграничения полномочий операторов с помощью парольного доступа. В зависимости от должности данного оператора, его опыта и квалификации ему могут назначаться определенные полномочия. Каждый оператор имеет возможность манипулирования системой строго в соответствии со своими полномочиями. Этим обеспечивается защита от взлома системы посторонними лицами и защита от неквалифицированного пользователя, так называемая "защита от дурака". Ограничения могут накладываться не только на возможность внесения изменений, но и на просмотр определенных разделов базы данных. Имеется возможность деления списка карт на группы с присвоением оператору прав доступа к каждой группе отдельно, что особенно важно для предприятий, сдающих помещения в аренду нескольким организациям.

Возможность варьировать цену системы на основе ПК APACS за счет использования оборудования с разным техническим уровнем, применение широкого спектра комплектующих известных производителей в составе единого комплекса - все это обеспечивает гибкость при создании реальных систем как в части их возможностей, так и в части цены. Например, можно использовать в качестве охранных панелей оборудование компании APOLLO различной степени секретности.

**2.3 Интегрированная система контроля с открытой архитектурой OnGuard 2000**

**2.3.1 Открытая архитектура**

Система безопасности, имеющая действительно открытую архитектуру, должна отвечать двум основным критериям:

* она должна быть разработана в соответствии со стандартами, используемыми в компьютерной индустрии;
* система должна легко интегрироваться с другими приложениями, программами и устройствами.

Как правило, крупные корпорации, предприятия могут использовать различные базы данных на корпоративном, региональном или ведомственном уровнях. Для того чтобы система была действительно открытой, она должна поддерживать как минимум несколько широко используемых стандартных баз данных, включая Oracle, SQL Server и т.п. Чтобы достигнуть этого уровня поддержки, система должна использовать стандарт ODBC (Open DataBase Connectivity), для чего необходим стандартный драйвер ODBC, что и предлагают многие производители систем безопасности. Однако поддержка ODBC на уровне базы данных -этого недостаточно. Поддержка ODBC должна осуществляться и на уровне приложения. Другими словами, приложения системы безопасности должны работать с различными типами баз данных, и, кроме того, производитель системы безопасности обязан провести тестирование своего программного обеспечения с различными типами баз данных.

Система с открытой архитектурой должна уметь работать с существующими стандартами сетей. На сегодняшний день TCP/IP является основным стандартом сетей, который поддерживают многие устройства. Однако система с открытой архитектурой должна поддерживать подключение смешанного оборудования, включая другие сетевые стандарты, такие как NetBios, IPX и HTTP. Кроме того, система с действительно открытой архитектурой должна поддерживать подключение множества устройств, таких как принтеры пропусков, видеооборудование, цифровые камеры и т.п. Практически это означает, что система должна поддерживать все Windows-совместимые устройства, использующие стандартные драйверы Win32.

**2.3.2 ИСБ – OnGuard 2000**

Основное направление компании Lenel - это разработка и построение полной интегрированной системы безопасности (ИСБ) путем интеграции различных технологий через открытую архитектуру.

ИСБ OnGuard 2000 отвечает всем требованиям, относящимся к системам с открытой архитектурой. ИСБ OnGuard 2000 объединяет в себе контроль доступа, печать пропусков, мониторинг тревог, контроль за перемещением имущества, цифровую видеозапись и управление, а также мониторинг с помощью браузера через Internet/Intranet. Кроме того, OnGuard 2000 поддерживает многосерверную архитектуру и уникальную технологию синхронизации баз данных. ИСБ OnGuard 2000 состоит из нескольких программных модулей, которые в сумме предоставляют максимальную защиту, оптимальную гибкость, простоту в управлении за приемлемую цену на одной программной платформе.

**2.3.3 Неограниченная емкость системы**

OnGuard 2000 предлагает неограниченное расширение системы контроля доступа под управлением одной интегрированной программной платформы. OnGuard 2000 разработана для инсталляций в компаниях разной величины: от систем на двух считывателях до больших транснациональных компаний, имеющих несколько зданий, тысячи считывателей, рассредоточенных по всему миру.

**2.3.4 Другие возможности OnGuard 2000**

OnGuard 2000 также имеет следующие возможности:

* детальные графические планы, с возможностью управления всеми точками доступа и тревожными точками, кроме того, поддерживаются все существующие графические форматы файлов, включая AutoCAD DXF;
* поддержка архитектуры вспомогательного (redundant) сервера базы данных, позволяющего продолжать работу системы в случае, если неисправен основной сервер;
* мощный генератор отчетов;
* широкие возможности интеграции с CCTV-оборудованием, пожарными панелями, интеркомом;
* поддержка управления лифтами и др. Существующие дополнительные программные модули OnGuard e-Administrator и OnGuard e-Visitor, с помощью которых можно организовать OnGuard JAVA Web Server, дают возможность администрирования и мониторинга системы безопасности из любой точки мира через Интернет с использованием обыкновенного браузера.

**2.4 ИСБ на базе ППКОП «Сфера 2001»**

"Сфера 2001" - первая российская адресно-аналоговая система пожарной сигнализации на базе извещателей и модулей серии 200/500 производства компании System Sensor. Протокол 200/500 -самый распространенный в мире, использующийся в ААСПС таких производителей как ESMI, Notifier, Honeywell, Ademco, Labor Strauss, FCI.

Преимущества адресно-аналоговых систем пожарной сигнализации:

* Раннее и точное обнаружение места пожара;
* Постоянный опрос каждого подключенного устройства;
* Настройка сигнала предварительной тревоги;
* Индивидуальная настройка чувствительности каждого извещателя (9 уровней);
* Возможность установки дневного и ночного режимов чувствительности извещателей;
* Контроль состояния каждого извещателя;
* Компенсация запыленности и предупреждение о необходимости обслуживания дымовых извещателей;
* Дистанционное тестирование извещателей с пульта управления;
* Сохранение работоспособности при обрыве или коротком замыкании на участке кольца;
* Экономия провода, быстрота монтажа и наладки.

Объединение в сеть нескольких приборов ППКОП "Сфера 2001" с выводом информации на компьютер позволяет создавать независимые подсистемы (пожарной сигнализации, управления противопожарной автоматикой, охранной сигнализации и т.д.) с аппаратной поддержкой интегрированной системы безопасности.

Каждый прибор "Сфера 2001" имеет сетевой контроллер.

Выходы контроллеров объединяются общим проводом и подключаются к компьютеру через специальный адаптер.

Для сохранения работоспособности системы при выходе из строя компьютера используются системные встроенные или выносные пульты управления приборами "Сфера 2001".

Высокая надежность интегрированных систем на базе ППКОП "Сфера 2001" определяется надежностью модулей прибора и оптимальным размером конфигурации прибора.

Оптимальный размер конфигурации прибора - 32 модуля в одном комплекте прибора "Сфера 2001", позволяет создавать на базе одного прибора любую из подсистем для здания средних размеров.

Применение однотипных модулей в различных подсистемах и доступная цена на модули (в частности на системный блок) - позволяет иметь на объекте систему "горячего" резервирования.

Реализации сети на аппаратном уровне:

* Приборы "Сфера 2001" объединяются в сеть с собственным протоколом;
* Длина сети до 10.000 м.

Модульная структура прибора и широкий выбор модулей позволяет создавать любую из подсистем ИС на базе однотипных приборов:

1 Адресно-аналоговую систему пожарной сигнализации;

2. Систему управления дымоудалением и противопожарной автоматикой;

3. Обычную систему пожарной сигнализации;

4. Систему охранной сигнализации;

5. Систему контроля доступа;

6. Систему автоматизации здания.

Большая длина адресных шлейфов прибора позволяет создавать сеть на значительной территории (в большом здании или в группе отдельно стоящих зданий).

Открытая архитектура ППКОП «Сфера 2001» позволяет интегрировать его, как на программном, так и на аппаратном уровне, с любыми приборами российского и зарубежного производства. Это делает наш прибор действительно универсальным - мы можем модернизировать уже существующее у Вас оборудование, сделав Вашу систему более надежной и функциональной при минимально возможных затратах.

Типовой размер конфигурации для различных систем на базе одного прибора "Сфера 2001":

* Адресно-аналоговая система пожарной сигнализации и управления дымоудалением и противопожарной автоматикой;
* 495 адресно-аналоговых датчиков;
* 495 модулей контроля и управления (контроль клапанов, шлейфы с обычными датчиками, реле для управления автоматикой, сирены и пр.);
* Обычная система пожарной сигнализации (512 шлейфов с обычными пожарными извещателями);
* 256 реле для управления автоматикой;
* Система охранной сигнализации (до 240 шлейфов с охранными извещателями);
* Система контроля доступа (20-40 дверей).

**2.4.1 Основные возможности прибора "Сфера 2001"**

Прибор «Сфера 2001» имеет следующие возможности:

* Подходит для больших и средних объектов, способен защитить объекты с большой территорией;
* Имеет модульную структуру, что позволяет легко наращивать систему;
* Сочетает надежность централизованного контроля и управления с достоинствами распределенных систем;
* Максимально снижает затраты на монтаж;
* Удобен и прост в эксплуатации;
* Снижает затраты на пуско-наладку и обучение пользователя;
* Имеет удобное меню на русском языке;
* Программируется с компьютера (бесплатное ПО на русском языке).

**2.4.2 Состав системы**

Система состоит:

* Более 1000 адресных устройств, в том числе: 495 адресно-аналоговых извещателей; 512 шлейфов с обычными извещателями; 256 индикаторов; 128 реле;
* 1000 пользователей для охранной сигнализации и СКД;
* Открытая архитектура, позволяющая легко интегрировать прибор в систему автоматизации зданий;
* Сеть из 31 прибора "Сфера 2001" с выходом на компьютер;
* Адресный шлейф длиной до 6000 метров;
* 30 модулей серии "Сфера 2001" включаются в адресный шлейф в любой комбинации;
* 3 реле и 7 зон сигнализации на базовом блоке;
* Встроенный или выносной системный пульт управления;
* Встроенный резервированный источник питания 24В 1,5А для питания модулей;
* 2 системных пульта с большим графическим дисплеем (16 строк по 32 символа);
* 4 объектовых пульта с большими символами (4 строки по 20 символов);
* Удобное, интуитивно понятное меню на русском языке и система подсказок;
* Управление основными функциями одним нажатием клавиши (сброс, выключение сирен, подтверждение тревоги, активизация тревоги);
* 4 уровня доступа для управления;
* 8 индикаторных панелей по 32 группы индикаторов (отображение состояния разделов: охрана, тревога, пожар, неисправность).

**Глава 3. Элементы интегрированной системы безопасности**

**3.1 Электрические измерения неэлектрических величин**

Современная электроизмерительная техника располагает совершенными и удобными в экспериментальном отношении методами измерений электрических величин, таких, как ток и напряжение, индуктивное, емкостное и омическое сопротивления электрической цепи, фаза и частота переменной э.д.с. и т.п. Благодаря существенным преимуществам электрических методов измерений (высокая точность и чувствительность, обеспечение дистанционности измерений и пр.) за последнее время все более широкое распространение получают косвенные методы измерений, заключающиеся в однозначном преобразовании измеряемой неэлектрической величины в электрическую с последующим определением последней.

Преобразование неэлектрических величин в электрические осуществляется с помощью устройств, принято называть датчика м и или преобразователями. Тип и конструкция датчика определяются необходимым преобразованием, т. е. преобразуемой входной неэлектрической и выходной электрической ведите а также условиями его работы.

Входными неэлектрическими величинами датчиков могут быть механические величины (линейные и угловые перемещения, скорость, ускорение, сила и моменты сил, упругость, частота колебаний, размеры, вес и объем различных тел), физические величины (температура, количество тепла, теплоемкость, тепловое сопротивление, магнитные свойства материала, цвет освещенность, световой поток, сила света, интенсивность излучения), химические величины (концентрация вещества и его количество) и органические величины (связанные с физиологическими процессами).

Выходными электрическими величинами датчиков обычно являются активное, индуктивное или емкостного сопротивления, ток, э. д. с. или падение напряжения, частота и фаза переменного тока.

Чувствительность датчиков с линейной зависимостью выходной величины от входной является величиной постоянной. У нелинейных датчиков чувствительность изменяется с изменением входной величины.

Датчик должен обеспечивать возможность получения непрерывной зависимости выходной величины от измеряемой входной, достаточную чувствительность и необходимую точность преобразования, необходимый диапазон изменений измеряемой величины, удобное согласование с измерительной аппаратурой. Он не должен оказывать существенного обратного влияния на измеряемую неэлектрическую величину и должен быть малоинерционным.

Электрическая величина на выходе датчика, характеризующая входную неэлектрическую величину, должна быть преобразована с помощью измерительной схемы в наиболее удобный для измерения вид. На выходе измерительной схемы электрическая величина измеряется с помощью измерителя, роль которого может выполнят электрический прибор или другое устройство, выполняющее измерительные функции. Таким образом, электрический прибор для измерения неэлектрической величины в общем случае состоит из датчика, измерительной и измерителя. Он может быть использован как самостоятельный прибор или же как составная часть системы автоматического регулирования различных процессов.

**3.1.1 Реостатные датчики**

Реостатный датчик представляет собой переменное сопротивление, подвижной контакт которого механически связан с объектом преобразуемого перемещения (линейного или углового). Выходной электрической величиной такого датчика является омическое сопротивление.

Часто реостатный датчик включается в электрическую цепь делителем напряжения. В этом случае его называют потенциометрическим датчиком. Выходной величиной такого датчика будет падение напряжения между подвижным и одним из неподвижных контактом.

Зависимость выходного напряжения от величины перемещения подвижного контакта соответствует закону изменения сопротивления вдоль потенциометра между неподвижным и подвижным контактами. У потенциометров с линейно изменяющимся сопротивлением выбор неподвижного контакта не влияет на закономерность изменения выходного напряжения. У потенциометров же с нелинейной закономерностью изменения сопротивления при смене положения неподвижного контакта меняется и закономерность изменения выходного напряжения датчика.

Достоинствами реостатных датчиков являются их высокая стабильность и точность преобразования, простота конструкции, малый вес и габариты, возможность питания постоянным и переменным током, простота регулировки. Наличие подвижного контакта ограничивает срок службы датчиков и ухудшает надежность их работы.

Реостатные датчики используются в системах автоматического регулирования, счетно-решающих и других устройствах, а также для измерения механических перемещений, геометрических размеров, уровня жидкостей и т. п.

интегрированная система безопасность авиапредприятие

**3.1.2 Проволочные датчики**

Принцип действия проволочных датчиков основан на свойстве металлической проволоки изменять свое сопротивление при ее растяжении внешней силой. При растягивании проволоки ее сопротивление изменяется за счет увеличения длины, уменьшения сечения и изменения удельного сопротивления.

Относительное изменение сопротивления проволоки датчика зависит от относительного удлинения этой проволоки .

Характеристика материалов, применяемых для изготовления проволочных датчиков:

1. Проволочные датчики изготовляются из тонкой проволоки (диаметром 0,02—0,05 мм) с высоким удельным сопротивлением. Конструктивно часто они представляют собой проволочную спираль наклеенную специальным клеем на тонкую бумагу, которая затем наклеивается на испытываемую деталь. Эти датчики применяются также в виде ненаклеенной спирали , струны и других конструкций.

2. Проволочные датчики используются при измерении малых перемещений, деформаций и вибраций (в манометрах, динамометрах, микрометрах и других аналогичных устройствах). Градуировка их производится с помощью эталонных деталей, зависимость упругих деформаций которых от прилагаемых сил известна. Из партии изготовленных датчиков отбирается несколько штук, и на градуировочной установке определяется их чувствительность. Затем подсчитывается средняя чувствительность, которая присваивается датчикам всей партии.

3. Ошибки преобразования с помощью проволочных датчиков обусловливаются зависимостью сопротивления проволоки датчика от температуры, нарушением крепления датчика на исследуемой детали и неточностью градуировки. Простейший метод компенсации температурных погрешностей проволочных датчиков состоит в том, что при преобразовании используются два датчика, которые включаются в смежные плечи мостовой измерительной схемы. При этом один из них наклеивается на испытываемую деталь, а другой не наклеивается, но оба они находятся в одинаковых температурных условиях. Изменение их сопротивления за счет окружающей температуры взаимно компенсируется в измерительной схеме. Точность преобразования проволочными датчиками составляет 1\_\_2%.

Достоинства проволочных датчиков заключаются в том, что они позволяют исследовать весьма малые перемещения (максимальное относительное удлинение не превышает 0,3—0,5%), имеют малые габариты и вес, практически безынерционны, легко принимают форму исследуемой детали. К недостаткам их следует отнести малое изменение сопротивления датчика при изменении преобразуемой величины (менее 1%), что приводит к необходимости применения в схемах с проволочными датчиками стабильных усилителей, сильную зависимость величины сопротивления от температуры окружающей среды, малую мощность рассеяния датчиком.

**3.1.3 Датчики контактного сопротивления**

Контактное сопротивление между поверхностями двух твердых тел зависит от величины давления одного тела на другое. Чем больше давление, тем меньше контактное сопротивление, и наоборот. Это явление используется в датчиках контактного сопротивления.

Контактное сопротивление между поверхностью твердых тел зависит также от материала этих тел и качества обработки соприкасающихся поверхностей. Наиболее существенные изменения контактного сопротивления при изменении давления происходят в случае использования в качестве таких тел электродных углей, удельное сопротивление которых Q = 30 ч- 100 ом-мм\м.

Датчики контактного сопротивления используются при исследовании различных механических давлений, , малых перемещений, вибраций, ускорений и в других, исследованиях. Наибольшее распространение они получили в качестве выходных органов регуляторов напряжения.

К недостаткам датчиков этого типа следует отнести зависимость их сопротивления от температуры и наличие гистерезиса. С целью компенсации температурного влияния применяются угольные датчики с двумя столбиками, которые включаются в смежные плечи мостовой схемы.

Термосопротивления.

В этом типе датчиков используется свойство проводника изменять свое электрическое сопротивление вменении его температуры. С помощью термосопротивления может быть осуществлено преобразование любой неэлектрической величины, влияющей на теплообмен проводника с окружающей средой, так как собственная температура термосопротивления определяется тепловым равновесием между ним и окружающей средой.

Материалом для термосопротивлении служат в основном металлы со сравнительно большим положительным температурным коэффициентом сопротивления (платина, никель, медь). Могут использоваться также и полупроводниковые материалы, имеющие более высокий температурный коэффициент сопротивления. Полупроводниковые термосопротивления (термисторы) имеют отрицательный температурный коэффициент.

В таблице1 указаны некоторые материалы, из которых изготовляются термосопротивления.

**Таблица 1** Проводниковые материалы, применяемые для изготовления термосопротивлении

|  |  |  |
| --- | --- | --- |
| Материал | Температурный коэффициент см° С | Удельное сопротивление ом-мм/м |
| Вольфрам Никель Платина Медь | 0,00421—0,00464 0,00621—0,00634 0,00394—0,0056 0,00433 | 0,055—0,0612 0,118—0,138 0,098—0,106 0,0156—0,017 |

Термосопротивления используются для измерения температур, для определения различных параметров газовой среды (скорость, вакуум, процентное содержание и т. д.).

Выбор материала термосопротивлення определяется условиями работы датчика и диапазоном рабочих температур. Медные термосопротивлення, например, могут хорошо работать в сухой атмосфере при отсутствии корродирующих газов в диапазоне изменения температур от -50 до +150° С. Никелевые термосопротивления требуют хорошей изоляции от воздействия внешней среды. Их можно применять для измерения температур до 250.

Платиновые термометры могут работать бея изоляции от внешней среды при температурах от -190 до +500° С. Через термосопротнвления, используемые в качестве термометров, должен протекать минимальный ток с тем чтобы нагрев термосопротивления за счет этого тока был наименьшим в сравнении с нагревом за счет испытуемой среды (обычно величина рабочего тока составляет 2-10 ма) Погрешности проволочных термометров сопротивления обусловливаются нестабильностью электрических свойств материала сопротивления, условиями применения (глубина погружения, теплопроводность держателя) и другими причинами. Точность современных термометров сопротивления (вместе с индикаторным прибором) составляет 1— 1.5%.

**3.1.4 Индуктивные датчики**

Действие индуктивных датчиков основано на свойстве катушки индуктивности изменять свое сопротивление при введении в нее ферромагнитного сердечника или при изменении величины зазора в магнитном сердечнике, на котором помещена катушка. Преобразуемой величиной в этом случае может быть механическое перемещение (линейное или угловое), а выходной величиной датчика — изменение индуктивности катушки.

Индуктивные датчики с подвижным сердечником внутри катушки используются для преобразования сравнительно больших перемещений (более 5— 8 мм). Датчики же с изменяющимся зазором магнитопровода служат для преобразования малых перемещений (до 2 мм при изменении длины зазора и до 8 мм при изменении его сечения).

Используются также двухтактные индуктивные датчики, обеспечивающие большой предел изменения преобразуемой величины, большую чувствительность и малую зависимость основных параметров датчика от внешних условий (температуры).

Широкое распространение получили трансформаторные датчики, представляющие собой устройства, в которых входное преобразуемое перемещение изменяет коэффициент взаимоиндукции между первичной и вторичной обмотками. Разновидностью их являются дифференциальные трансформаторные датчики с двумя вторичными обмотками см.рис.2 в приложении. Датчики этого типа позволяют получить более мощный выходной сигнал по сравнению с другими типами датчиков (например, проволочными) .

Погрешности индуктивных датчиков зависят от стабильности амплитуды и частоты питающего напряжения, а также от влияния окружающей температуры на геометрические размеры магнитопровода и датчика.

Индуктивные датчики применяются в основном для преобразования различных механических перемещений, исследования деформаций, контроля размеров и т. д. Динамические свойства индуктивных датчиков определяются инерционностью его подвижных элементов.

**3.1.5 Емкостные датчики**

Емкость конденсатора зависит от трех параметров:

* площади обкладок;
* расстояния между ними;
* диэлектрической постоянной среды между обкладками.

Принцип действия емкостного датчика основан на том, что преобразуемая неэлектрическая величина воздействует на один из указанных параметров, изменяя тем самым емкость конденсатора.

В соответствии с числом параметров, определяющих емкость конденсатора, различают три типа емкостных датчиков:

1. с изменяющейся площадью обкладок;

2. с изменяющимся расстоянием между обкладками;

3. с изменяющейся диэлектрической постоянной.

Конструктивные выполнения датчиков могут быть различными. Минимальное расстояние между обкладками выбирается из расчета диэлектрической прочности.

Чувствительность их очень высока; она превосходит чувствительность всех других типов датчиков. Погрешность емкостных датчиков определяется влиянием температуры на геометрические размеры и диэлектрическую проницаемость диэлектрика, а также влажностью окружающей среды.

Основными схемами включения емкостных датчиков являются мостовые и дифференциальные схемы, а также схемы, построенные на использовании явления резонанса и метода биений.

Емкостные датчики могут быть использованы для преобразования механических перемещений (линейных и угловых), геометрических размеров деталей, расстояний между деталями, состава физических смесей, вибраций, измерения уровня жидкостей и других величин.

**3.1.6 Магнитоупругие датчики**

Ферромагнитные материалы обладают двумя следующими свойствами:

* если брусок ферромагнитного материала подвергнуть намагничиванию, то его геометрические размеры (длина) изменятся;
* если намагниченный брусок ферромагнитного материала подвергнуть действию внешней силы, то его намагниченность (магнитная проницаемость) изменится.

Первое свойство называется магнитострикцией, а второе магнитоупругим эффектом. Действие магнитоупругих датчиков основано на явлении магнитоупругого эффекта.

Таким образом, входной величиной датчика может быть механическое усилие, а выходной — полное сопротивление катушки. При питании катушки датчика переменным током выходной величиной может быть амплитуда тока, протекающего через катушку.

Чувствительность магнитоупругого датчика зависит от магнитной чувствительности сердечника к давлению, а также от конструкции магнитопровода и катушки датчика. Конструкция датчика должна быть выполнена так, чтобы потоки рассеяния были сведены к минимуму. Наибольшей магнитной чувствительностью к давлению обладают магнитные материалы, имеющие большую магнитную проницаемость с большим значением магнитострикции при малой индукции насыщения. К ним относятся некоторые сорта пермаллоя а также трансформаторная сталь.

**3.2 Индукционные, термоэлектрические и пьезоэлектрические датчики**

**3.2.1 Индукционные датчики**

В индукционных датчиках используется Явление электромагнитной индукции, заключающееся в том, что в проводнике, перемещаемом в магнитном поле перпендикулярно направлению магнитных силовых линий, наводится э. д. с, пропорциональная скорости движения проводника (аналогично наводится э. д. с. при перемещении магнитного поля относительно проводника или же при изменении интенсивности магнитного поля вокруг проводника).

Индукционные датчики непосредственно могут применяться только для измерения скорости линейных и угловых перемещений (тахогенераторы). Особые конструкции тахогенератора позволяют измерять ускорения вращающихся валов.

Конструктивно датчики выполняются либо с катушкой, перемещаемой в неподвижном магнитном поле, либо с перемещаемым магнитным полем и неподвижной катушкой, либо с неподвижными катушкой и магнитным полем, но перемещаемым прерывателем магнитного потока.

Для повышения чувствительности индукционных датчиков, выходной величиной которых является частота, необходимо изготовлять их с большим числом пар магнитных полюсов.

Для измерения скорости вращения или скорости возвратно-поступательного движения могут применяться импульсные датчики, основанные на явлении электромагнитной индукции. Выходной величиной таких датчиков является частота следования импульсов. Такой датчик представляет собой постоянный магнит, укрепленный на подвижном объекте, и сигнальную катушку, укрепляемую неподвижно.

Другой разновидностью импульсного датчика может быть такой датчик, у которого неподвижной является система из постоянного магнита, магнитопровода и сигнальной катушки; в качестве подвижной части используется диск из ферромагнитного материала с отверстиями.

Погрешности индукционных датчиков определяются:

1) изменениями магнитного поля с течением времени (эта погрешность устраняется периодической регулировкой магнитного шунта);

2) изменениями сопротивления обмоток и силы магнитного поля за счет нагрева (эта погрешность устраняется применением термомагнитного шунта или термистора в цепи якоря). Погрешность их может быть сведена к величине 0,5—1,5%.

**3.2.2 Термоэлектрические датчики (термопары)**

Принцип действия термоэлектрических датчиков основан на явлении термоэлектрического эффекта, заключающегося в том, что если два разнородных проводника соединить одними концами в одной точке и место соединения нагреть, то на свободных «холодных» концах проводников появится э. д. с. Величина этой э. д. с. зависит от материалов, из которых изготовлены элементы термопары, и от разности температур соединенных и свободных концов.

Для термоэлектрических датчиков выбирают такие сочетания термоэлектродов, которые дают наибольшие значения термо-э. д. с. К материалам, используемым для изготовления электродов термопар, предъявляются следующие требования:

1. механическая и химическая устойчивостьпри высокихтемпературах;

2. хорошая электропроводность;

3. постоянство термоэлектрических свойств;

4. однозначная зависимость термо-э. д. с. от температуры.

Для измерения температур до 1000° С включительно используются термопары из неблагородных металлов. Температуры до 1600° С измеряются термопарами из благородных металлов. Свыше 1600° С используются термопары из жароупорных материалов: уголь — карбид кремния (до 1800° С); вольфрам—молибден (до 2100° С).

Предельная температура применения термопары зависит не только от свойств ее электродов, но и от конструкции приемной части датчика (армировки), длительности применения и свойств среды, в которой работает термопара.

Свободные концы электродов термопары соединяются с измерителем посредством проводов. Если материал соединительных проводов и материалы электродов термопары разнородны, то в местах соединения будут создаваться термо-э. д. с, величины которых зависят от температуры среды, окружающей выводы термопары.

Термо-э. д. с, наведенные на свободных («холодных») концах термопары, алгебраически складываются с основной термо-э. д. с, характеризующей измеряемую температуру, и тем самым вносят соответствующие искажения в измерения. При постоянстве температуры среды, окружающей головку с выводными зажимами, эти искажения могут быть учтены при градуировке термопары.

Если температура головки термопары изменяется, то погрешности измерения за счет термо-э. д. с, наводимых на выходных зажимах, не могут быть учтены при градуировке. В таких случаях к измерителю термопары придается график поправок на измерение в зависимости от температуры головки (зажимов измерителя) или же применяются специальные схемы соединения термопары с измерителем.

Инерционность термопар определяется их конструкцией, условиями теплообмена с окружающей средой. Постоянная времени термопар может находиться в пределах единиц до нескольких сотен секунд.

**3.2.3 Обращенные датчики**

Принцип действия обращенных датчиков основан на сравнении двух неэлектрических величин, одна из которых измеряемая, а другая получена путем преобразования известной электрической величины. Эти датчики используются главным образом как измерители.

Неоновая лампа периодически зажигается импульсами напряжения, вырабатываемыми блокинг-генератором. При совпадении частоты вспышек с частотой следования меток, нанесенных на вращающемся объекте, последний будет казаться неподвижным. Зная частоту блокинг-генератора, можно определить частоту вращения объекта.

Другим примером обращенного преобразователя является электрооптический пирометр, служащий для измерения высоких температур.

Обращенные преобразователи применяются в качестве звеньев обратной отрицательной связи при построении высокоточных измерительных устройств неэлектрических величин.

**3.3 Усиление сигналов датчика**

В электрических приборах для измерения неэлектрических величин находят широкое применение различного рода усилители, которые служат для согласования выходов датчиков и мостовых схем с измерительными приборами или устройствами, выполняющими измерительные функции. При этом осуществляется усиление сигналов датчиков или мостовых схем по току или напряжению:

Часто с выхода датчиков или мостовых измерительных схем снимаются постоянные по величине или медленно изменяющиеся сигналы, которые должны быть усилены. Для этого широко используются так называемые усилители постоянного тока. Среди них различают усилители с непосредственной связью между каскадами и усилители с преобразованием постоянного сигнала в переменный.

Усилители с непосредственной связью выполняются без переходных емкостей с непосредственной гальванической связью выхода предыдущего каскада с выходом последующего.

В усилителях с преобразованием входной сигнал постоянного тока или напряжения преобразуется в переменное напряжение, амплитуда которого пропорциональна величине входного сигнала. Усиление преобразованного сигнала осуществляется усилителями переменного тока.

Для получения неискаженного сигнала на выходе усилителя необходимо обеспечить нормальные режимы работы ламп (или транзисторов) и стабильность его параметров в течение всего времени работы.

Обеспечение необходимых режимов работы ламп может быть достигнуто применением отдельных источников питания для каждого каскада или потенциометрических Делителей с общим источником питания.

Применение отдельных источников питания для каждого каскада неудобно, так как усилительная установка получается громоздкой. Поэтому такой способ питания применяется главным образом в лабораторной практике.

Достижение необходимой стабильности работы усилителей с непосредственной связью может быть обеспечено применением стабилизированных источников питания, специальных компенсирующих схем и отрицательной обратной связи. Для питания анодных цепей усилителей применяются выпрямители с электронной стабилизацией или гальванические элементы. В меньшей степени, но также необходима стабилизация питания накала ламп.

Обычно стабилизация источников питания все же оказывается недостаточной. Поэтому наряду с ней применяют специальные схемы усилителей.

Применение отрицательной обратной связи улучшит характеристики усилителя. При этом уменьшаются нелинейные, частотные и фазовые искажения. Влияние нестабильности источников питания также становится меньшим.

**3.4 ИК-пассивные датчики охранной системы**

Датчики являются одним из главных элементов системы сигнализации и во многом определяют ее эффективность. Анализ номенклатуры датчиков, предлагаемых крупнейшими производителями систем охранной сигнализации, показывает, что в классе датчиков для охраны помещений наиболее популярными являются инфракрасные (ИК) пассивные, комбинированные (в основном ИК+микроволновые), различные модификации контактных (в первую очередь магнитоконтактные) и акустические датчики разбития стекла. Реже применяются микроволновые, ультразвуковые, активные и инерционные ударные датчики.

Ниже рассматриваются принципы действия, номенклатура и особенности применения наиболее популярных датчиков охранной сигнализации - ИК-пассивных. Эти датчики предназначены в первую очередь для защиты объема охраняемого помещения.

ИК-пассивные датчики, называемые также оптико-электронными, относятся к классу детекторов движения и реагируют на тепловое излучение движущегося человека Принцип действия этих датчиков основан на регистрации изменения во времени разницы между интенсивностью ИК излучения от человека и фонового теплового излучения В настоящее время ИК-пассивные датчики являются самыми популярными, они составляют неотъемлемый элемент охранной системы практически каждого объекта. Для того чтобы нарушитель был обнаружен ИК-пассивным датчиком, необходимо выполнение следующих условий:

* нарушитель должен пересечь в поперечном направлении луч зоны чувствительности датчика;
* движение нарушителя должно происходить в определенном интервале скоростей; чувствительность датчика должна быть достаточной для регистрации разницы температур поверхности тела нарушителя (с учетом влияния его одежды) и фона (стены, пол) ИК-пассивные датчики состоят из трех основных элементов:

а) оптической системы, формирующей диаграмму направленности датчика и определяющей форму и вид пространственной зоны чувствительности;

б) пироприемника, регистрирующего тепловое излучение человека;

в) блока обработки сигналов пироприемника, выделяющего сигналы, обусловленные движущимся человеком, на фоне помех естественного и искусственного происхождения.

В ИК-датчиках, предназначенных для профессионального использования, применяются так называемые схемы антимаскинга. Суть проблемы состоит в том, что обычные ИК-датчик могут быть выведены нарушителем из строя путем предварительного (когда система не поставлена на охрану) заклеивания или закрашивания входного окна датчика. Для борьбы с этим способом обхода ИК-датчиков и используются схемы антимаскинга Метод основывается на использовании специального канала ИК-излучения, срабатывающего при появлении маски или отражающей преграды на небольшом расстоянии от датчика (от 3 до 30 см). Схема антимаскинга работает непрерывно, пока система снята с охраны. Когда факт маскирования обнаруживается специальным детектором, сигнал об этом подается с датчика на контрольную панель, которая, однако, не выдает сигнала тревоги до тех пор, пока не придет время постановки системы на охрану. Именно в этот момент оператору и будет выдана информация о маскировании. Причем, если это маскирование было случайным (крупное насекомое, появление крупного объекта на некоторое время вблизи датчика и т.п.) и к моменту постановки на сигнализацию самоустранилось, сигнал тревоги не выдается.

Еще одним защитным элементом, которым оборудованы практически все современные ИК-детекторы, является контактный датчик вскрытия, сигнализирующий о попытке открывания или взлома корпуса датчика. Реле датчиков вскрытия и маскирования подключаются к отдельному шлейфу охраны.

**3.4.1 Установка и использование ИК-датчиков**

При выборе типов и количества датчиков для обеспечения охраны конкретного объекта следует учитывать возможные пути и способы проникновения нарушителя, требуемый уровень надежности обнаружения; расходы на приобретение, монтаж и эксплуатацию датчиков; особенности объекта; тактико-технические характеристики датчиков Особенностью ИК-пассивных датчиков является их универсальность - с их использованием возможно блокирование от подхода и проникновения самых разнообразных помещений, конструкций и предметов: окон, витрин, прилавков, дверей, стен, перекрытий, перегородок, сейфов и отдельных предметов, коридоров, объемов помещений. При этом в ряде случаев не потребуется большого количества датчиков для защиты каждой конструкции - может оказаться достаточным применения одного или нескольких датчиков с нужной конфигурацией зоны чувствительности. Остановимся на рассмотрении некоторых особенностей применения ИК-датчиков.

К ложным срабатываниям ИК-датчиков могут привести помехи теплового, светового электромагнитного, вибрационного характера. Несмотря на то, что современные ИК-датчики имеют высокую степень защиты от указанных воздействий, все же целесообразно придерживаться следующих рекомендаций:

* для защиты от потоков воздуха и пыли не рекомендуется размещать датчик в непосредственной близости от источников воздушных потоков (вентиляция, открытое окно);
* следует избегать прямого попадания на датчик солнечных лучей и яркого света; при выборе места установки должна учитывается возможность засветки в течение непродолжительного времени рано утром или на закате, когда солнце низко над горизонтом, или засветки фарами проезжающего снаружи транспорта;
* на время постановки на охрану целесообразно отключать возможные источники мощных электромагнитных помех, в частности источники света не на основе ламп накаливания: люминесцентные, неоновые, ртутные, натриевые лампы;
* для снижения влияния вибраций целесообразно устанавливать датчик на капитальных или несущих конструкциях; не рекомендуется направлять датчик на источники тепла (радиатор, печь) и колеблющиеся предметы (растения, шторы), в сторону нахождения домашних животных.

**3.5 Магнитоконтактные и электроконтактные датчики**

Контактные датчики относятся к самым простым. Обычно они устанавливаются на двери и окна охраняемого помещения. Среди контактных датчиков широкое применение нашли электроконтактные датчики, представляющие собой ленту из тонкой алюминиевой фольги. Она клеится на стекло, двери, стены и т. п. При разрушении основания, на которое наклеена лента, она рвется и разрывает электрическую цепь. Для подключения к шлейфу охранной сигнализации лента зажимается в держателе (клемме), который приклеивается к тому же основанию, что и лента.

Широко распространены контактные датчики магнитного типа (магнитоконтактные датчики). Эти датчики выпускаются двух типов: для наружной и скрытой установки. Для повышения надежности охраны часто устанавливают по два и более датчиков, которые соединяют между собой последовательно. Магнитоконтактные датчики, предназначенные для скрытой установки, имеют цилиндрическую форму. Эти датчики, как и электроконтактные, подключаются к проводным шлейфам охранной сигнализации.

**3.6 Радиоволновые и комбинированные детекторы движения**

Радиоволновые детекторы движения предназначены для обнаружения и регистрации движения в охраняемой зоне. Каждый детектор содержит СВЧ-модуль, в состав которого входят излучатель и приемник высокочастотных колебаний. В отличие от пассивных ИК детекторов, подробно рассмотренных выше, радиоволновые детекторы являются активными устройствами, так как излучают в пространство СВЧ колебания. Принцип действия этих приборов основывается на интерференции радиоволн сантиметрового диапазона или эффекте Доплера (изменение частоты принимаемого сигнала, отраженного от движущегося объекта).

При охране внутренних помещений по характеристикам радиоволновые детекторы аналогичны описанным выше пассивным ИК детекторам. Однако в отличие от них, они имеют более низкую помехозащищенность и достаточно высокий уровень СВЧ излучений. Поэтому в последнее время все чаще стали применяться приборы, в состав которых входят два детектора - пассивный ИК и радиоволновый. Это так называемые детекторы двойной технологии. В таких приборах пассивный ИК детектор работает непрерывно. При регистрации им факта движения теплового объекта в зоне обнаружения включается радиоволновый детектор. Если последний подтвердит наличие подвижного объекта в зоне охраны, прибор сформирует и выдаст по шлейфу сигнализации тревожное извещение путем замыкания или размыкания контактов выходных реле. Такой режим работы детекторов позволяет обеспечить высокий уровень помехозащищенности прибора и уменьшить уровень СВЧ излучений, поскольку радиоволновый детектор включается только на короткое время.

Радиоволновые детекторы могут работать на одной из нескольких рабочих частот (литер), устанавливаемых с помощью переключателей на плате СВЧ-модуля прибора. Это позволяет использовать несколько однотипных детекторов, работающих на различных частотных литерах, в одном помещении одновременно.

**3.7 Системы ограждений и охранные извещатели**

Эффективность и надежность охраны протяженных рубежей важных объектов в современных условиях могут быть обеспечены лишь на основе оптимального сочетания различных сигнальных и сигнально-заградительных средств обнаружения (извещателей), а также глухих, транспарантных (просматриваемых) и комбинированных ограждений (заграждений), объединенных в комплексы технических средств сигнализации при помощи специальной кабельной сети. Подобные комплексы должны обеспечиваться гарантированным электропитанием и связью с системами сбора и обработки информации, средствами управления доступом на объект.

Грамотное комбинирование средств обнаружения различных физических принципов действия позволяет, как правило, добиться выполнения важнейших требований, предъявляемых к охранной сигнализации. При последующем изложении под "рубежом охраны" будем понимать условные линию или поверхность, ограничивающие разнообразные объекты охраны, как-то:

* территорию;
* область пространства;
* комплекс здании или отдельные здания, сооружения, помещения, отдельные предметы и т п., в то время как в методических рекомендациях НИЦ "Охрана" ГУВО МВД фигурирует понятие "рубеж охранной сигнализации", обозначающее совокупность совместно действующих технических средств охранной сигнализации, последовательно объединенных электрической цепью, позволяющих выдать извещение о проникновении (попытке проникновения) в охраняемую зону (зоны), не входящих в данную цепь. В настоящее время наиболее широкое (по протяженности оборудованных рубежей) применение в составах сигнализационных комплексов получили электроконтактные (электромеханические), емкостные, индуктивные, вибрационные, радиоволновые (радиолучевые) СО.

Для обеспечения сигнализационного блокирования протяженных рубежей и периметров важных объектов в каждом конкретном случае приходится решать ,комплекс похожих задач, оптимизировать сочетание механических препятствий, прежде всего ограждений, со средствами сигнализации - механические препятствия призваны затруднять и замедлять проникновение нарушителя на время, необходимое для его раннего обнаружения средствами сигнализации Для прохода персонала через ограждения при регламентных работах (на ограждениях и на составных элементах ТСОС), а также для удаления растительности с внешней стороны блокируемого рубежа проектируются калитки в ограждениях и их сигнализационное блокирование. В отдельных случаях могут устраиваться переходы (шлюзы), оборудованные средствами управления доступом.

В тексте проекта ГОСТ Р "Средства систем охраны и безопасности. Термины и определения дано определение ограждения (сооружение или конструкция, применяемые для выгораживания территории или ее части) и констатируется, что ограждения могут быть следующих видов:

* глухое ограждение - ограждение, не просматриваемое насквозь;
* транспарантное ограждение - ограждение, просматриваемое насквозь;
* комбинированное ограждение - ограждение, обладающее сочетанием свойств ограждений различных типов.

Таким образом, при комплексировании извещателей и ограждений должны быть учтены следующие соображения:

* необходимость оптимизации тактико-технических характеристик (вероятность обнаружения, наработка на ложное срабатывание, наработка на отказ, имитостойкость) при максимально возможной помехоустойчивости;
* необходимость оборудования проходов в ограждениях (ворот и калиток) и сигнализационного блокирования их;
* обеспечение надежного электроснабжения и качественного заземления аппаратуры;
* организация грозозащиты;
* разумная прокладка кабельных линий**.**

**3.7.1 Понятие извещателя**

Начиная говорить об извещателях нужно в первую очередь сказать что такое извещение.

Изещением в технике охранно-пожарных сигнализаций (ОПС) называется сообщение несущее информацию о контролируемых изменениях состояния охранного объекта или технических средств ОПС и передаваемое с помощью электромагнитных, электрических, световых или звуковых сигналов.

Извещения делятся на тревожные и служебные:

* Тревожное извещение содержит информацию и проникновении (попытке проникновения) или пожаре;
* служебное о "взятии" под охрану, "снятии" с охраны, неисправности аппаратуры и др.

В отличие от датчиков извещатель представляет собой простейшую охранную систему он содержит все необходимые технические средства охранно-пожарной сигнализации, датчик, устройство обработки информации, поступающей от датчика, устройство ввода информации, как правило, в одном корпусе.

Сигнал, формирующий извещение является индикатором состояния прибора.

Отдельные извещатели можно использовать как автономные системы сигнализации, но чаще их используют в качестве "сложных" датчиков в составе технических средств охранно-пожарной сигнализации. Охранные извещатели являются первичными техническими средствами обнаружения проникновения или попытки проникновения в охраняемую зону.

Охранно-пожарные извещатели дополнительно к охранной функции способны обнаруживать физические факторы, сопровождающие пожар - открытое пламя, дым.

**3.7.2 Выбор типа извещателя**

Выбор того или иного типа извещателя производится с учетом множества факторов:

* климатических условий;
* конструктивных параметров охраняемого объекта;
* вероятных путей проникновения;
* режимной тактики охраны;
* требований дизайна;
* степени надежности охраны.

Выбор конкретного типа извешатедя производится в первую очередь с учетом особенностей защищаемого объекта, таких как его площадь и объем, тип горючей загрузки, климатических условий, наличие воздушных потоков и прочего

**Таблица 2** Область применения извещателей

|  |  |  |
| --- | --- | --- |
| Блокируемая конструкция | Способ воздействия | Тип извещателя |
| Окна, витрины, стеклянные прилавки.двери со стеклянным полотном, рамы, фрамуги, форточки | Открывание, разрушение стекла (разбиение стекла и вырезание), проникновение | Магнитоконтактный, омический, ударноконтактные, звуковые, пьезоэлектрические, пассивные оптико-электронные, эадиоволновые, комбинированные |
| Двери, ворота, погрузочно-разгрузочные люки | Открывание, пролом, проникновение | магнитоконтактные, выключатели оконечные, активные оптико-электронные, омический провод, пьезоэлектрические, пассивные оптико-электронные, радиоволновые, ультразвуковые, комбинированные |
| Оконные решётки, решётчатые двери, решётки дымоходов | Открывание, перепиливание | Магнитоконтактные для мета-лических конструкций, омический поовод |
| Стены, полы, потолки, перекрытия.перегородки, места ввода коммуникаций | Пролом, проникновение | Омический провод, пьезоэлектрические, вибрационные, активные линейные, оптико-электронные, пассивные оптико-электронные, радиоволновые, ульрозвуковые, комбини-пованные |

|  |  |  |
| --- | --- | --- |
| Сейфы, отдельные Предметы | Разрушение (ударные воздействия, пиление, сверление), касание, приближение, проникновение (подход к защищаемым предметам) | пьезоэлектрические, виброционные, емкостные, оптико-электронные, радиоволновые, ультрозвуковые, комбинированные |
| Коридоры | Проникновение | Оптико-электронные, радиоволновые, комбиниоованные |
| Объём помещений | Проникновение | Пассивные оптико-электронные, радиоволновые |
| Внешний периметр, открытые площадки | Проникновение | Активные линейные оптико-электронные, радиоволновые |

**3.7.3 Классификация извещателей**

По способу формирования информационного сигнала от проникновения нарушителя или пожара извещатели делятся на:

• активные - излучают в охраняемой зоне сигнал и реагируют на изменение его параметров,

• пассивные - реагируют на сигнал, создаваемый нарушителем или пожаром.

Отдельные группы извещателей подразделяются также по принципу действия чувствительного элемента, например: ударноконтактные, пьезоэлектрические, пироэлектрические фотодиодные.

По способу передачи информации на центральный пульт или транслятор извещатели делятся на:

• проводные;

• радиоканальные.

По устойчивости к воздействию внешних климатических факторов извещатели делятся на:

• предназначенные для отапливаемых помещений;

• для неотапливаемых помещений;

• для наружной установки.

По способу электропитания извещатели делятся на:

* непотребляющие (пассивные);
* питающиеся от шлейфа сигнализации;
* питающиеся от автономного источника питания;
* питающиеся от низковольтного (12 - 24 В) вторичного источника питания;
* питающиеся от сети переменного тока 220 В 50 Гц.

По дальности ультразвуковые, оптико-электронные и радиоволновые извещатели для закрытых помещений различают:

* малой дальности т.е. область их действия до 12м;
* средней дальности от 12 до 30 м;
* большой дальности более 30 м.

По конструктивному исполнению ультразвуковые, оптико-электронные и радиоволновые подразделяют на:

* однопозиционные - передатчик (излучатель) и приёмник установлены совместно в одном блоке (может быть несколько передатчиков и приёмников в одном блоке);
* двухпозиционные - передатчик и приёмник расположены в различных блоках;
* многопозиционные - более двух блоков (передатчики и приёмники в любых комбинациях).

**3.7.4 Принципы работы извещателей**

В извещателях используется различные физические принципы обнаружение в охраняемой зоне нарушителя или пожара:

* Электроконтактный - размыкание или замыкание электрической цепи;
* Параметрический - изменение параметров электростатического поля, пар; метров электрической цепи (емкость, индуктивность, электрическое сопротивление);
* Вибрационный - возникновение или изменение параметров упругих колебаний в твердых телах (стекло, металл, бетон, кирпич, древесина и пр.);
* Акустический - возникновение или изменение параметров упругих колебаний в воздушной среде (от инфра до ультразвуковых частот);

**3.8 Свойства извещателей серии 200 и 500**

Свойства извещателей:

* В извешателе имеется два светодиодных индикатора (СИД) для отображения состояния тревоги. Сработавший извешатель виден со всех сторон (угол зрения 360°);
* Легко осуществляется профилактическое тестирование и извешателя при помощи магнита. В каждом извещателе имеется встроенный контур для тестирования, активация которою происходит при помощи магнита, подносимого к наружной поверхности извета геля;
* Извещатель прост в обслуживании, не вызывает трудностей;
* Извещатель имеет надежную защит) от ложных сообщений, вызываемых пылью, насекомыми и перепадами давления;
* Извещатель устойчив к потокам воздуха;
* Параллельно к извещателю можно подключишь сигнализаторы;
* Сигнал о необходимости технического обслуживания загрязненного извещателя;
* При нахождении щита «F.SA» в состоянии профилактического обслуживания возможен контроль за загрязнением извещателя;
* Измерение чувствительности извешателя осуществимо без отсоединения извещателя от цоколя, при помощи специального тестера непосредственно в полевых условиях;
* При помощи программы конфигурации UTHra «ESA» возможна установка уровня чувствительности для каждого извешателя в отдельности;
* Простая установка адреса каждою извещателя;
* С извешателями данной серии используется один тин монтажного цоколя;
* Извещатель может быть блокирован на цоколе;
* В поставку входит пластмассовый кожух, защищающий извещатель от пыли, возникающей в ходе производства строительных работ;
* Азотные извещатели серий 200 и 500 производят постоянный контроль за происходящими изменениями и посылают о них сообщения на шит «ЕSA» дальнейшего принятия решения.

**Выводы и рекомендации**

1. ИСБ универсальна, она способна собирать максимум информации и дает возможность менять алгоритм ее обработки в зависимости от складывающейся ситуации, что крайне важно для авиапредприятия как объекта с высокой степенью технической оснащенности средствами безопасности. При использовании ИСБ в целях повышения уровня авиационной безопасности решается комплекс проблем, которые влияют на безопасность авиапредприятия
2. ИСБ рекомендуется применять на базе комплексных систем, так как она способна включать в свой состав неограниченное число подсистем. Именно интегрированные системы безопасности предназначены для борьбы не только с «внешними», но и с «внутренними» врагами (перекрытие каналов утечки информации) и имеют для этого широкий спектр специальных возможностей.
3. Подробно рассмотренные чувствительные элементы (датчики ИСБ), базирующихся на использовании физических законов позволяет выбрать датчики многофункционального типа, регистрирующих одновременно несколько параметров, что является экономически выгодным при использовании 2-3 датчиков.
4. Следует сказать, что существующая в настоящее время номенклатура сигнализационных датчиков, а также достигнутые ими тактико-технические характеристики при правильном выборе и грамотном проектировании смогут обеспечить надежную и эффективную защиту.

**Список используемой литературы**

1. Учебное пособие, СПб, Академия ГА 1997 г. «Обеспечение авиационной безопасности в авиапредприятиях ГА», Никулин Н. Ф.;
2. «Системы безопасности», журнал для специалистов в области безопасности, январь 2002 №42;
3. «Системы безопасности», журнал для специалистов в области безопасности, май 2005 №48;
4. «Справочник радиолюбителя», Куликовский А. Н., 1977;
5. Журнал: БДИ, безопасность, достоверность, информация январь, февраль 1998г.
6. Журнал: системы безопасности, связи и телекоммуникаций ноябрь-декабрь 1998г.
7. Межотраслевой тематический каталог системы безопасности 1999г.
8. Математические методы решения задач для создания ИСБ.
9. Учебные пособия по данной проблематике.
10. С.В. Кошелев, Г.А. Клауз, В.В. Гвоздецкий «Монтаж и наладка систем производственной электрической связи, сигнализации и электрочасофикации». Учебник для техникумов. Москва «Радио и связь» 1991г.
11. Журнал: Системы охраны и теленаблюдения Москва 2002-2003 г.