Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ №1(32)/1997

ОФИЦИАЛЬНАЯ ХРОНИКА

Международная конференция и тематическая выставка "Безопасность информации"

В апреле 1997 года в Москве будет проводиться Международная конференция и тематическая выставка «Безопасность информации». Компания «Инфосистемы Джет» является информационным спонсором данного мероприятия.

Вниманию читателей Jet Info предлагается подборка официальных материалов о конференции и выставке, предоставленных пресс-центром Гостехкомиссии России.

Информационное сообщение

15 октября 1996 года состоялось очередное заседание Государственной технической комиссии при Президенте Российской Федерации.

Одним из вопросов, обсужденным на этом заседании было рассмотрение предложений Гостехкомиссии России, ФАПСИ, Центробанка России, Российской инженерной академии и Федеральной академии экономической безопасности о проведении с 14 по 18 апреля 1997 года в Москве Международной конференции и тематической выставки «Безопасность информации».

Инициатива проведения такой конференции поддержана членами Гостехкомиссии России. На заседании одобрены Концепция проведения Международной конференции, Регламент и основные мероприятия по ее подготовке.

Состав Организационного комитета одобрен Правительством Российской Федерации. Заместитель Председателя Правительства Российской Федерации О.И. Лобов дал согласие возглавить национальный организационный комитет. Его заместителями определены Председатель Государственной технической комиссии при Президенте Российской Федерации Ю.А. Яшин, Генеральный директор Федерального агентства правительственной связи и информации при Президенте Российской Федерации А.В. Старовойтов, Председатель комитета при Президенте Российской Федерации по политике информатизации А.С. Голубков.

В состав Оргкомитета вошли представители министерств и ведомств, государственных и коммерческих банков, научных и общественных организаций.

Международная конференция проводится с целью создания условий для эффективного творческого взаимодействия представителей всех групп пользователей информации, заинтересованных в обеспечении ее безопасности, выработки концептуальных и методологических положений для повышения эффективности решения этих задач, прогнозирования тенденций развития методологических и научно-практических основ безопасности информации и обмена передовым опытом работы.

На конференции планируется работа секций: правовые аспекты безопасности информации; безопасность банковской информации; лицензирование деятельности в области защиты информации, современные средства защиты информации и их сертификация; информационные аспекты экономической безопасности; безопасные информационные технологии; подготовка и переподготовка кадров.

Пресс-центр Гостехкомиссии России 18 октября 1996 г.

Замысел подготовки и проведения Международной конференции «Безопасность информации» и тематической выставки

Цель проведения Международной конференции:

- Создание условий для эффективного творческого взаимодействия представителей всех групп пользователей информации, заинтересованных в обеспечении ее безопасности.
- Выработка концептуальных и методологических положений для повышения эффективности решения задач обеспечения безопасности информации.
- Разработка практических рекомендаций и предложений по усилению безопасности информации.
- Прогнозирование тенденций развития методологических и научно-практических основ безопасности информации.
- Обмен передовым опытом работы по обеспечению безопасности информации.

Цели проведения тематической выставки:

- Выявление перспективных образцов и технических решений аппаратуры защиты информации.
- Содействие продвижению лучших образцов отечественной аппаратуры на внутренний и мировой рынок.

Учредители Конференции и выставки:

- Государственная техническая комиссия при Президенте Российской Федерации;
- Федеральное Агентство правительственной связи и информации при Президенте Российской Федерации;
- Центральный банк Российской Федерации;
- Государственный комитет Российской Федерации по науке и технологиям;
- Российская инженерная академия;
- Федеральная академия экономической безопасности.

Секции Конференции:

- Правовые аспекты безопасности информации (компьютерное право; правовые основы регулирования деятельности в области защиты информации; законодательство по проблемам защиты информации; законодательство по вопросам международного обмена информацией; законодательство по вопросам интеллектуальной собственности; нормативно-методическая база безопасности информации);
- Безопасность банковской информации (обеспечение защиты конфиденциальной информации в кредитно-финансовых учреждениях; банковские технологии обработки информации; средства защиты информации);
- Лицензирование деятельности в области защиты информации, современные средства защиты информации, их сертификация (угрозы безопасности информации, современные технологии защиты информации, в том числе при интеграции в глобальные телекоммуникационные сети; охрана корпоративных интересов; обеспечение тайны связи; системы сертификации; нормативно-методическая база сертификации; сертификация общесистемного программного обеспечения зарубежного производства; развитие добровольной сертификации; аттестация производства средств защиты информации и объектов информатизации);
- Информационные аспекты экономической безопасности (экономические интересы и безопасность информации; безопасность информации и самостоятельная внешнеэкономическая деятельность субъектов Федерации, финансово-промышленных групп и других субъектов хозяйствования; безопасность информации при использовании фискальной памяти контрольно-кассовых аппаратов, тарификаторов, POS-терминалов и т.д.; сертификация средств защиты информации устройств с фискальной памятью; защита экономической информации в автоматизированных системах);
- Безопасные информационные технологии (методы и средства разработки программного обеспечения; его тестирование и оценка безопасности; защита информации от программно-математических воздействий);
- Подготовка и переподготовка кадров по специализации «Защита информации» (подготовка и переподготовка специалистов служб безопасности информации; специалистов в области технических средств комплексной защиты информации; в области законодательства по вопросам безопасности информации).

Форма проведения Конференции:

- Пленарные заседания (в первый и последний день работы Конференции).
- Секционные заседания.
- "Круглые столы"
- Межсекционные тематические заседания.
- Пресс-конференции.

Конференция проводится за счет организационных взносов учредителей и участников.

Окончание – см. стр 20
Конференция

Вячеслав Барсуков
кандидат технических наук,
РАО "Газпром"

Физическая защита информационных систем

Содержание

1. Введение

Характерной тенденцией развития информационных технологий является процесс тотальной интеграции. Этой тенденцией охвачены микроэлектроника и техника связи, сигналы и каналы, системы и сети. В качестве примеров можно сослаться на сверхбольшие интегральные схемы, интегральные сети передачи данных, многофункциональные устройства связи и т.п.

Наряду с интеграцией функциональной, схемотехнической и системной, в последнее время стала активно развиваться интегральная информационная безопасность (ИИБ). Под интегральной безопасностью понимается такое состояние условий функционирования человека, объектов и технических средств, при котором они надежно защищены от всех возможных видов угроз в ходе непрерывного процесса подготовки, хранения, передачи и обработки информации.

Интегральная безопасность информационных систем включает в себя следующие составляющие:

- физическая безопасность (защита зданий, помещений, подвижных средств, людей, а также аппаратных средств — компьютеров, носителей информации, сетевого оборудования, кабельного хозяйства, поддерживающей инфраструктуры);
- безопасность связи (защита каналов связи от внешних воздействий любого рода);
- безопасность программного обеспечения (защита от вирусов, логических бомб, несанкционированного изменения конфигурации);
- безопасность данных (обеспечение конфиденциальности, целостности и доступности данных).

Так сложилось, что хронологически первой стала развиваться физическая безопасность, а уже потом — другие разделы информационной безопасности. Однако в последнее время развитие методов и технических средств обеспечения физической безопасности обрело новый импульс.

Учитывая это, в данной работе предпринята попытка рассмотреть различные аспекты физической безопасности с позиций интегрального подхода. Основное внимание уделено анализу современных методов и технических средств обеспечения физической безопасности, направленных на защиту объектов, информации и физических лиц.

2. Основы рассматриваемого подхода

Задача обеспечения информационной безопасности стара как мир. Она появилась вместе с проблемой передачи и хранения информации. На современном этапе можно выделить три подхода к ее решению:

- первый (частный) подход основывается на решении частных задач обеспечения информационной безопасности. Этот подход является малоэффективным, но достаточно часто используется, так как не требует больших финансовых и интеллектуальных затрат.
- второй (комплексный) подход основывается на решении комплекса частных задач по единой программе. Этот подход в настоящее время является основным.
- третий (интегральный) подход основан на интеграции различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных.

Третий подход направлен на достижение интегральной информационной безопасности. Понятие интегральной безопасности предполагает обязательную непрерывность процесса обеспечения безопасности как во времени, так и в пространстве (по всему технологическому циклу деятельности) с обязательным учетом всех возможных видов угроз (несанкционированный доступ, съем информации, терроризм, пожар, стихийные бедствия и т.п.).

Интегральный подход к проблеме информационной безопасности, безусловно, является наиболее перспективным, однако его применение невозможно без развитой инфраструктуры, значительных материальных и интеллектуальных затрат и высокого уровня технических средств. Эти обстоятельства сдерживают развитие интегральной безопасности. В настоящее время на практике встречаются все три подхода к обеспечению информационной безопасности, причем используются они как самостоятельно, так и в различных сочетаниях, что позволило создать, например, охранно—пожарные, тревожные и другие системы малого уровня интеграции.

В какой бы форме ни применялся интегральный подход, он связан с решением ряда сложных разноплановых частных задач в их тесной взаимосвязи. Наиболее очевидными из них являются задачи ограничения доступа к информации, технического и криптографического закрытия информации, ограничения уровней паразитных излучений технических средств, технической укрепленности объектов, охраны и оснащения их тревожной сигнализацией. Однако, необходимы решения и других, не менее важных задач. Так, например, выведение из строя руководителей предприятия, членов их семей или ключевых работников может поставить под сомнение само существование данного предприятия. Этому же могут способствовать стихийные бедствия, аварии, терроризм и т.п.

Первым шагом в создании системы физической безопасности (как и информационной безопасности вообще) должен стать анализ угроз (рисков), как реальных (действующих в данный момент), так и потенциальных (могущих возникнуть в будущем).

По результатам анализа рисков с использованием средств оптимизации формируются требования к системе безопасности конкретного предприятия и объекта в конкретной обстановке. Завышение требований приводит к неоправданным расходам, занижение — к возрастанию вероятности реализации угроз.

В общем случае система физической безопасности должна включать в себя следующие подсистемы:

- управления доступом (с функцией досмотра);
- обнаружения проникновения, аварийной и пожарной сигнализации (тревожной сигнализации);
- инженерно—технической защиты (пассивной защиты);
- отображения и оценки обстановки;
- управления в аварийных и тревожных ситуациях;
- оповещения и связи в экстремальных ситуациях;
- личной безопасности персонала.

При построении системы физической безопасности, удовлетворяющей сформулированным требованиям, разработчик выбирает и объединяет средства противодействия из числа указанных ниже:

- здания и строительные препятствия, мешающие действиям злоумышленника и задерживающие его;

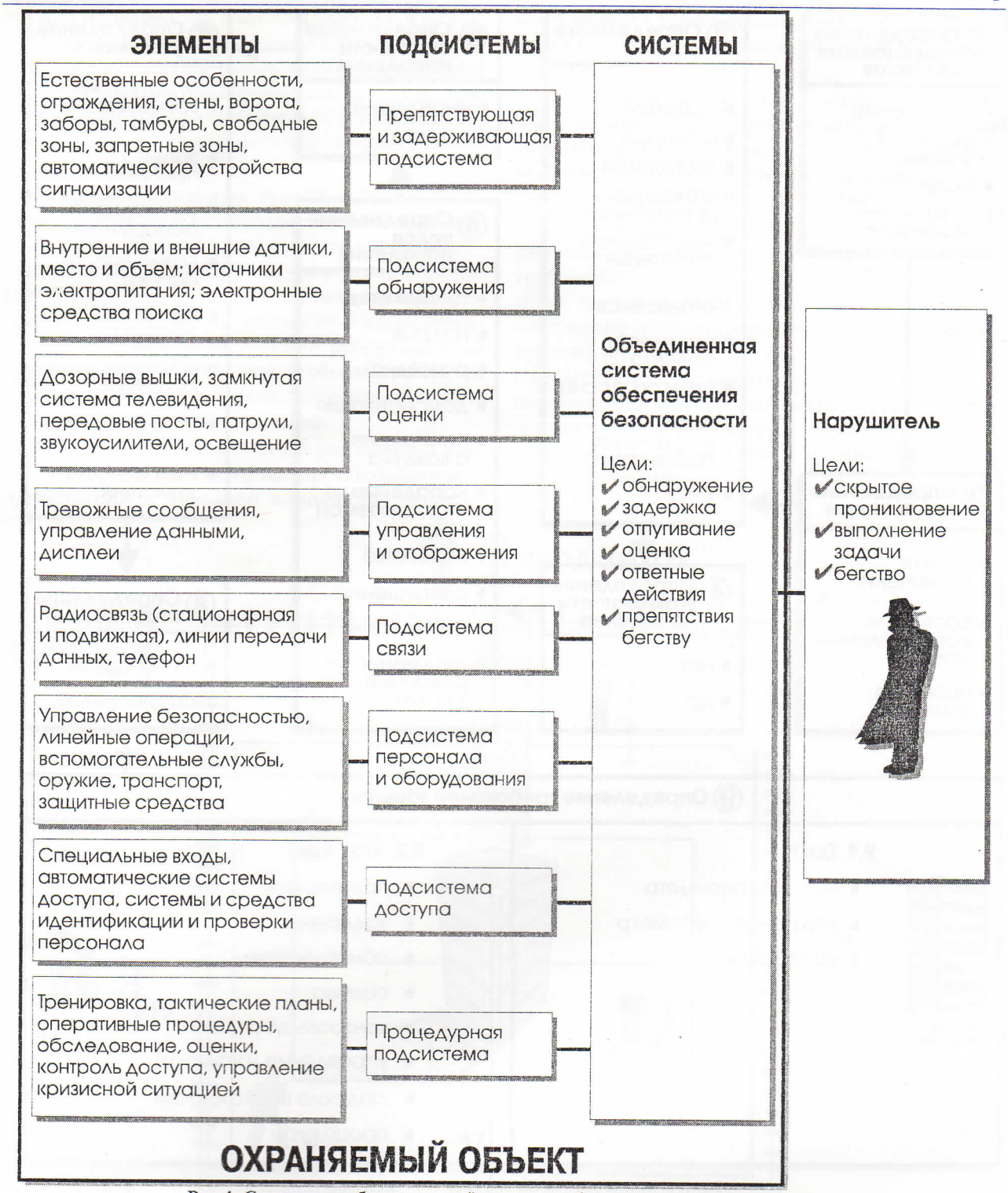

Рис.1. Структура объединенной системы обеспечения безопасности.

- аппаратура тревожной сигнализации, обеспечивающая обнаружение попыток проникновения и несанкционированных действий, а также оценку их опасности;
- системы связи, обеспечивающие сбор, объединение и передачу тревожной информации и других данных;
- системы управления, необходимые для отображения и анализа тревожной информации, а также для реализации ответных действий оператора и управления оборонительными силами;
- персонал охраны, выполняющий ежедневные программы безопасности, управление системой и ее использование в нештатных ситуациях;
- процедуры обеспечения безопасности, предписывающие определенные защитные мероприятия, их направленность и управление ими.

На рис. 1 представлены технические средства противодействия и соответствующие подсистемы, имеющиеся в распоряжении разработчика.

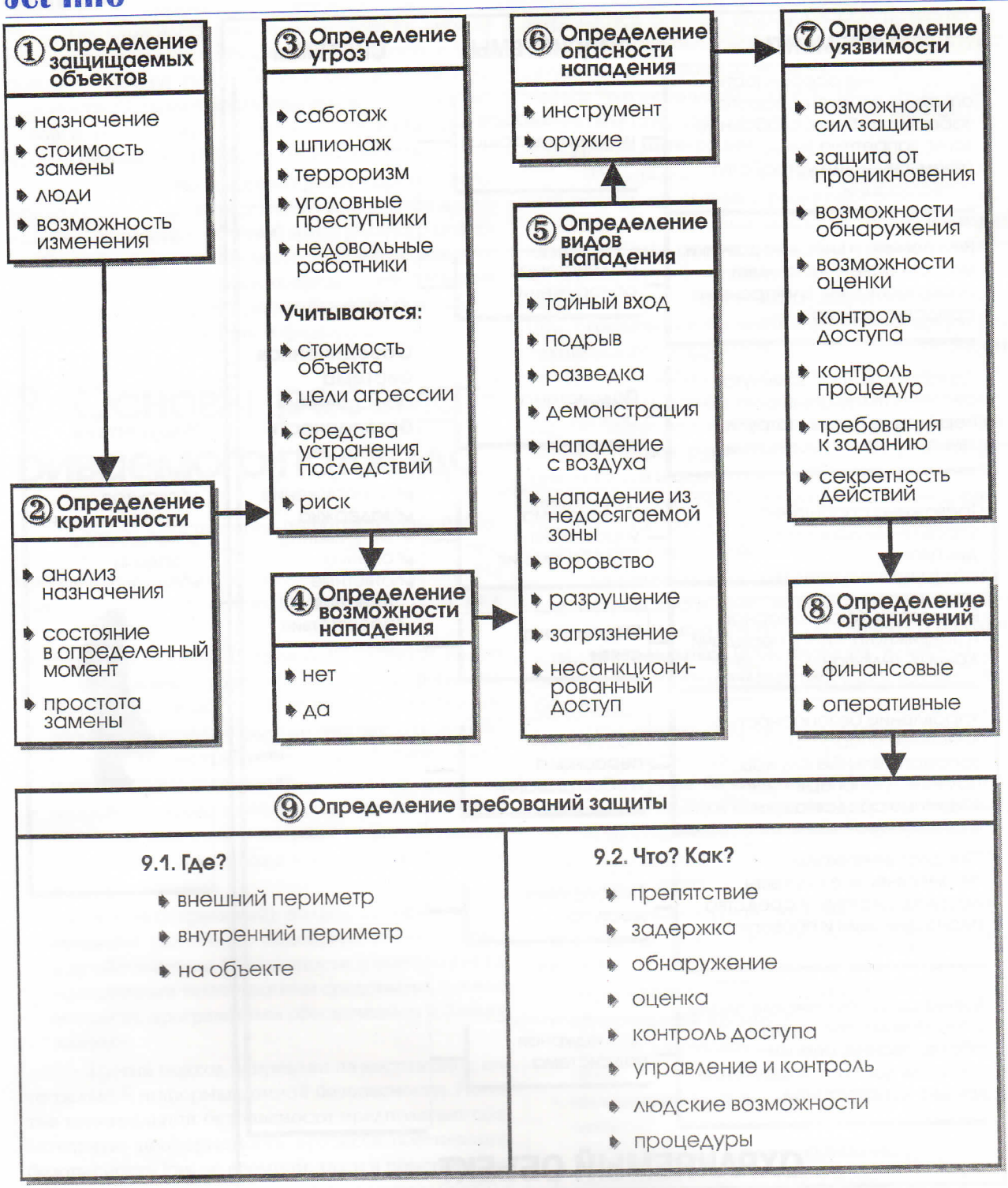

Рис.2. Процесс выбора средств противодействия.

Как показывает опыт, успешная разработка системы безопасности возможна только в том случае, когда процесс выбора средств противодействия и объединения их в единую систему разделен на этапы и определены соответствующие каждому этапу задачи. На рис. 2 этот процесс представлен в графической форме.

Первоначально определяются объекты, которые надо защитить, и их функции. Затем оценивается степень интереса потенциального противника к этим объектам, вероятные виды нападения и вызываемый ими ущерб. Наконец, определяются уязвимые для воздействия области, в которых имеющиеся средства противодействия не обеспечивают достаточной защиты.

Для эффективного применения процесс выбора средств противодействия должен содержать оценку каждого объекта с точки зрения возможных угроз и видов нападения, потенциальной вероятности применения специальных инструментов,

оружия и взрывчатых веществ (этапы 3 и 4 на рис. 2). Особо важным допущением в этом процессе является предположение о том, что наиболее ценный для потенциального злоумышленника объект привлечет наибольшее внимание и будет служить вероятной целью, против которой злоумышленник использует основные силы.

Разработка средств противодействия должна соответствовать концепции полной и эшелонированной защиты. Это означает, что средства противодействия следует размещать на концентрических кругах, пересекающих все возможные пути противника к любому объекту. Рис. 3 иллюстрирует данную концепцию. Каждый рубеж обороны организуется таким образом, чтобы задержать нападающего на время, достаточное для принятия персоналом охраны ответных мер.

На заключительном этапе разработчик объединяет выбранные средства противодействия в соответствии с принятой концепцией защиты. Производится также предварительная оценка начальной и ожидаемой общей стоимости жизненного цикла всей системы.

Разработчик должен принимать во внимание такое понятие, как жизненный цикл защищаемых объектов. В частности, он должен учитывать возможные перемещения объектов, а также изменение требований в местах входа.

В том случае, когда внутри одного здания располагаются объекты с существенно разными требованиями к безопасности, применяется разделение здания на отсеки, что позволяет выделить внутренние периметры внутри общего контролируемого пространства и создать внутренние защитные средства от несанкционированного доступа. Периметр обычно выделяется физическими препятствиями, проход через которые контролируется электронным способом или с помощью специальных процедур.

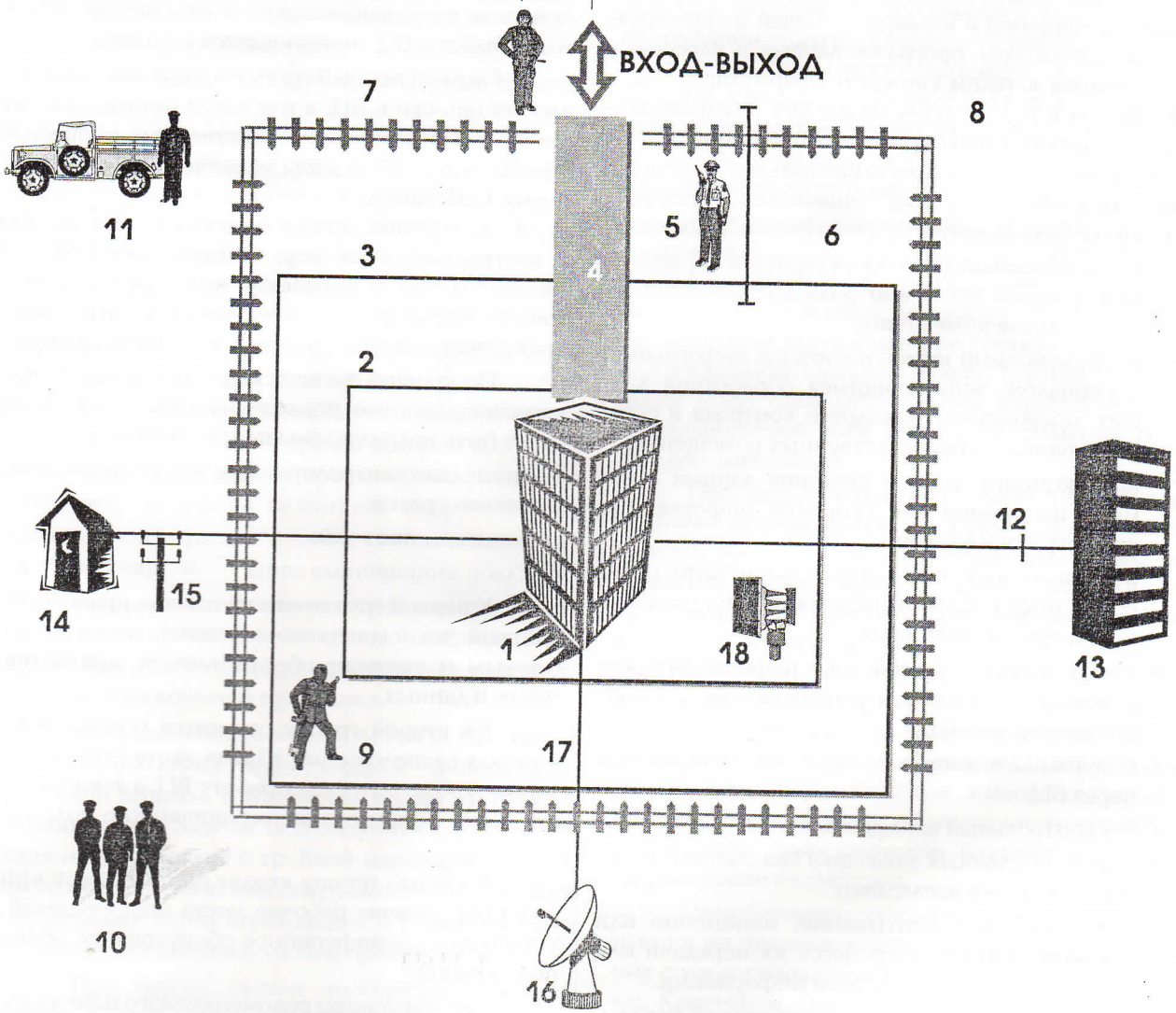

Рис.3. Элементы классической системы обеспечения безопасности (охраны) объекта:
1 – охраняемый объект; 2 – задерживающее ограждение; 3 – обнаруживающее ограждение; 4 -контролируемый вход; 5 – зона оценки; 6 – нейтральная зона; 7 – забор; 8 – дальняя защита; 9 – силы внутренней обороны; 10 – силы внешней обороны; 11 – подвижный патруль; 12 – канал связи; 13 – внешний объект; 14 – электроподстанция; 15 – линия электропередачи; 16 – объекты технического обеспечения; 17 – инженерные коммуникации; 18 – радиосигнализация.

При защите группы зданий, имеющих общую границу или периметр, необходимо учитывать не только отдельный объект или здание, но и место, на котором они расположены. Обычно участки местности с большим количеством зданий имеют общие или частично совпадающие требования по обеспечению безопасности, а некоторые участки имеют ограждение по периметру и единую проходную. Организация общего периметра позволяет уменьшить количество защитных средств в каждом здании и устанавливать их только для наиболее важных объектов или зданий, нападение на которые наиболее вероятно. Аналогичным образом, каждое строение или объект на участке следует оценить с точки зрения их возможностей задержать нападающего.

С учетом вышеизложенного рассмотрим в качестве примера проблему защиты вычислительных центров.

Надежная система должна обеспечивать защиту помещений и поддерживающей инфраструктуры, аппаратуры, программ, данных и персонала. Требования к таким системам сформулированы, в частности, в федеральном законе ФРГ по охране данных. Закон содержит перечень из девяти требований к защите, которые следует выполнять путем осуществления соответствующих технических и организационных мероприятий. Должны быть исключены:

- неправомочный доступ к аппаратуре обработки информации путем контроля доступа в производственные помещения;
- неправомочный вынос носителей информации персоналом, занимающимся обработкой данных, посредством выходного контроля в соответствующих производственных помещениях;
- несанкционированное введение данных в память, изменение или стирание информации, хранящейся в памяти;
- неправомочное пользование системами обработки информации и незаконное получение в результате этого данных;
- доступ в системы обработки информации посредством самодельных устройств и незаконное получение данных;
- возможность неправомочной передачи данных через ВЦ;
- бесконтрольный ввод данных в систему;
- обработка данных заказчика без соответствующего указания последнего;
- неправомочное считывание, изменение или стирание данных в процессе их передачи или транспортировки носителей информации.

Анализ перечисленных требований показывает, что они сводятся к исключению возможности неправомочного доступа к устройствам обработки и передачи информации, похищения носителей информации и проведения актов саботажа. Данные требования могут быть выполнены путем осуществления комплекса мероприятий полицией, администрацией ВЦ и специальными уполномоченными по охране информации.

Разработку концепции защиты рекомендуется проводить в три этапа. На первом этапе должна быть четко определена целевая установка защиты, то есть установлено, какие реальные ценности, производственные процессы, программы, массивы данных необходимо защищать. На этом этапе целесообразно проводить дифференциацию по значимости отдельных объектов, требующих защиты.

На втором этапе должен быть проведен анализ видов преступных действий, которые потенциально могут быть совершены в отношении ВЦ. Важно определить степень реальной опасности таких наиболее широко распространенных категорий преступлений, как экономический шпионаж, терроризм, саботаж, кражи со взломом. Затем необходимо проанализировать наиболее вероятные действия злоумышленников в отношении основных объектов ВЦ, нуждающихся в защите.

Главной задачей третьего этапа является анализ обстановки в ВЦ, в том числе местных специфических условий, производственных процессов, уже установленных в ВЦ технических средств защиты. Собственно концепция защиты должна содержать перечень организационных, технических и других защитных мер, которые обеспечивают максимальную безопасность при заданном остаточном риске и при минимальных затратах на практическое осуществление этих мероприятий.

По уровню физической защиты все зоны и производственные помещения современных ВЦ могут быть подразделены на три группы:

- тщательно контролируемые зоны с защитой высокого уровня;
- защищенные зоны;
- слабо защищенные зоны.

К первой группе относятся, как правило, машинный зал (серверные комнаты), помещения с сетевым и связным оборудованием, архив программ и данных.

Ко второй группе относятся помещения, в которых расположены рабочие места администраторов, контролирующих работу ВЦ, а также периферийное оборудование ограниченного пользования.

В третью группу входят помещения, в которых оборудованы рабочие места пользователей и установлено периферийное оборудование общего пользования.

Таковы основы рекомендуемого нами подхода. Далее будут рассмотрены технические средства, позволяющие этот подход реализовать.

3. Комплексная защита объектов

Современный комплекс защиты территории охраняемых объектов должен включать в себя следующие основные компоненты:

- механическую систему защиты;
- систему оповещения о попытках вторжения;
- оптическую (обычно телевизионную) систему опознавания нарушителей;
- оборонительную систему (звуковую и световую сигнализацию, применение в случае необходимости оружия);
- связную инфраструктуру;
- центральный пост охраны, осуществляющий сбор, анализ, регистрацию и отображение поступающих данных, а также управление периферийными устройствами;
- персонал охраны (патрули, дежурные на центральном посту).

3.1. Механические системы защиты

Основой любой механической системы защиты являются механические или строительные элементы, создающие для лица, пытающегося проникнуть на охраняемую территорию, реальное физическое препятствие. Важнейшей характеристикой механической системы защиты является время сопротивления, то есть время, которое требуется злоумышленнику для ее преодоления. Исходя из требуемой величины названной характеристики должен производиться и выбор типа механической системы защиты.

Как правило, механическими или строительными элементами служат стены и ограды. Если позволяют условия, могут применяться рвы и ограждения из колючей проволоки.

Вышеназванные элементы могут сочетаться в различных комбинациях в одной системе механической защиты. В настоящее время на ценных охраняемых объектах используются системы механической защиты с тройной изгородью, со специальными элементами, затрудняющими попытки перелезания через ограждения, и с применением S — образных мотков колючей проволоки.

При использовании многорядных механических систем защиты датчики оповещения о попытке вторжения целесообразно располагать между внутренним и внешним ограждением. При этом внутреннее ограждение должно обладать повышенным временем сопротивления.

3.2. Системы оповещения

В современных системах оповещения (системах тревожной сигнализации) о попытках вторжения на охраняемую территорию находят применение датчики нескольких типов. Поскольку основные характеристики подобных систем определяются, главным образом, характеристиками используемых датчиков, рассмотрим принципы действия и особенности применения последних более подробно.

В системах защиты периметра территории без ограды используются микроволновые, инфракрасные, емкостные, электрические и магнитные датчики.

С помощью датчиков первых двух типов формируется протяженная контрольная зона барьерного типа. Действие систем с микроволновыми датчиками основывается на контроле интенсивности высокочастотного направленного излучения передатчика, которое воспринимается приемником. Срабатывание сигнализации происходит при прерывании этого направленного излучения. Ложные срабатывания могут быть обусловлены перемещением в контролируемой зоне животных, воздействием растительности, атмосферных осадков, передвижением транспортных средств, а также воздействием посторонних передатчиков.

При использовании инфракрасных систем оповещения между передатчиком и приемником появляется монохроматическое световое излучение в невидимой области спектра. Срабатывание сигнализации происходит при прерывании одного или нескольких световых лучей. Ложные срабатывания могут быть обусловлены перемещением в контролируемой зоне животных, сильным туманом или снегопадом.

Принцип действия емкостной системы оповещения основывается на формировании электростатического поля между параллельно расположенными, так называемыми, передающими и воспринимающими проволочными элементами специального ограждения. Срабатывание сигнализации происходит при регистрации определенного изменения электростатического поля, имеющего место при приближении человека к элементам ограждения. Ложные срабатывания могут быть обусловлены перемещением животных, воздействием растительности, обледенением элементов ограждения, атмосферными воздействиями или загрязнением изоляторов.

Электрические системы оповещения базируются на использовании специального ограждения с токопроводящими проволочными элементами. Критерием срабатывания сигнализации является регистрация изменений электрического сопротивления токопроводящих элементов при прикосновении к ним. Ложные срабатывания могут быть вызваны животными, растительностью или загрязнением изоляторов.

Принцип действия систем с магнитными датчиками предполагает контроль параметров магнитного поля. Срабатывание сигнализации происходит при регистрации искажений, которые обусловлены появлением в зоне действия датчиков предметов из ферромагнитного материала. Ложное срабатывание может иметь место из—за изменений характеристик почвы, обусловленных, например, продолжительным дождем.

При наличии механической системы защиты территории (например, ограды, расположенной по периметру) находят применение системы оповещения с вибрационными датчиками, датчиками звука, распространяющегося по твердым телам, акустическими датчиками, электрическими переключателями, а также системы с электрическими проволочными петлями.

Вибрационные датчики закрепляются непосредственно на элементах ограды. Срабатывание сигнализации происходит при появлении на выходе датчиков сигналов, которые обусловлены вибрациями элементов ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем или градом.

Датчики звука также устанавливаются непосредственно на элементы ограды и контролируют распространение по ним звуковых колебаний. Срабатывание сигнализации происходит при регистрации так называемых шумов прикосновения к элементам ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем, градом или срывающимися с элементов ограды сосульками.

В системах оповещения с акустическими датчиками контролируются звуковые колебания, передаваемые через воздушную среду. Срабатывание сигнализации происходит при регистрации акустических сигналов, имеющих место при попытках перерезать проволочные элементы ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем, градом, а также различными посторонними шумами.

Действие систем с электрическими переключателями основано на регистрации изменения состояния переключателей, вмонтированных в ограду, которое происходит при соответствующем изменении натяжения проволочных элементов или нагрузки на направляющие трубки ограды. Ложные срабатывания сигнализации могут быть вызваны очень сильным ветром при недостаточном натяжении элементов ограды.

Если в системах оповещения в качестве чувствительных элементов применяются изолированные токопроводящие проволочные элементы, срабатывание сигнализации происходит при перерезании или деформации этих элементов. Ложные срабатывания могут произойти при возникновении неисправности в сети электропитания.

Для контроля участков почвы по периметру охраняемой территории находят применение системы оповещения с датчиками звука, распространяющегося по твердым телам, а также с датчиками давления.

В системах первого типа регистрируются звуковые, сейсмические колебания. Срабатывание сигнализации происходит при регистрации сотрясений почвы, например, ударного шума. Ложные срабатывания могут быть обусловлены перемещением достаточно крупных животных, движением транспорта вблизи охраняемой территории.

В системах второго типа используются пневматические или емкостные датчики давления, позволяющие регистрировать изменения нагрузки на почву. Срабатывание сигнализации происходит при регистрации соответствующего роста давления, например, ударного. Ложные срабатывания возможны из—за перемещений достаточно крупных животных, разгерметизации пневматических датчиков или коррозии.

Для контроля участков охраняемой территории фирмой Multisafe AG разработана система оповещения Multiplain, датчики которой работают на принципе регистрации разности давления. Необходимо отметить, что названный физический принцип до настоящего времени не использовался для обнаружения попыток вторжения на охраняемую территорию. Датчик состоит из двух полых тел с избыточным давлением, которые соединены между собой через специальный преобразователь разности давлений. При возникновении даже незначительной разницы давлений в этих телах в преобразователе срабатывает контакт, через который может коммутироваться цепь включения тревожной сигнализации.

При использовании указанного датчика достаточно просто локализовать участок, на котором сработал чувствительный элемент. Кроме того, преобразователь оснащен устройством автоматического восстановления нулевой точки, что исключает срабатывание контакта при медленных изменениях давления, которые могут быть обусловлены различными возмущающими воздействиями, например, колебаниями температуры. Датчик также нечувствителен к колебаниям и вибрациям, обусловленным движением автомобильного или железнодорожного транспорта.

Чувствительная часть рассматриваемого устройства конструктивно выполнена в виде набора специальных ковриков, которые могут устанавливаться под слоем гравия, дерна, земли или под плитами пешеходных дорожек. Срабатывание контактов в преобразователях происходит при изменении нагрузки не менее чем на 30 кг. Таким образом, система оповещения не реагирует на перемещение мелких животных по контролируемому участку территории. Предварительная нагрузка за счет мас-

кировочного покрытия ковриков может достигать 250 кг/м² без влияния на их чувствительность.

Приведенное описание позволяет сделать вывод об отсутствии идеальной системы оповещения. Основное техническое требование к подобной системе может быть сформулировано следующим образом: максимально возможная вероятность обнаружения и надежность в сочетании с минимальной частотой ложных срабатываний.

Повышение вероятности обнаружения нарушителя системой оповещения обязательно сопровождается увеличением числа ложных срабатываний. Таким образом, разработка систем оповещения связана, прежде всего, с поиском рационального компромисса относительно соотношения величин названных показателей. Из этого следует, что дальнейшее совершенствование систем оповещения должно обеспечить прежде всего повышение вероятности обнаружения и снижение интенсивности ложных срабатываний путем использования нескольких систем оповещения различного принципа действия в едином комплексе и применения в этих системах микропроцессорных анализаторов.

3.3. Системы опознавания

Обязательным условием надежного функционирования всего комплекса защиты охраняемой территории является последующий анализ поступающих сообщений о проникновении для точного определения их вида и причин появления. Названное условие может быть выполнено посредством использования систем опознавания.

Наиболее широкое распространение в подобных системах получили телевизионные установки дистанционного наблюдения. Несомненно, что объект со стационарными постами охраны обладает более высокой защищенностью, однако при этом значительно возрастают затраты на его охрану. Так, при необходимости круглосуточного наблюдения требуется трехсменная работа персонала охраны. В этих условиях телевизионная техника становится средством повышения эффективности работы персонала охраны, прежде всего при организации наблюдения в удаленных, опасных или труднодоступных зонах.

Вся контролируемая системой оповещения зона разграничивается на отдельные участки протяженностью не более 100 м, на которых устанавливается по крайней мере одна передающая телекамера. При срабатывании датчиков системы оповещения, установленных на определенном участке контролируемой зоны, изображение, передаваемое соответствующей телекамерой, автоматически выводится на экран монитора на центральном посту охраны. Кроме того, при необходимости должно быть обеспечено дополнительное освещение данного участка. Немаловажно, чтобы внимание дежурного охранника было быстрее привлечено к выведенному на экран монитора изображению.

Фактические причины срабатывания сигнализации во многих случаях могут быть идентифицированы только при условии достаточно высокой оперативности дежурного охранника. Важно, что данное положение прежде всего имеет место при действительных попытках вторжения на охраняемую территорию и при преднамеренных обманных действиях злоумышленников. Одним из перспективных путей выполнения вышесформулированного условия является применение устройства видеопамяти, которое обеспечивает автоматическую запись изображения сразу же после срабатывания сигнализации. При этом дежурному охраннику предоставляется возможность вывести из устройства памяти на экран монитора первые кадры изображения и идентифицировать причину срабатывания датчиков системы оповещения.

В ряде телесистем наблюдения применены передающие камеры, ориентация которых может дистанционно меняться дежурным охранником. При включении сигнализации тревоги служащий охраны должен ориентировать телекамеру на участок, где сработали датчики системы оповещения. Практический опыт показывает, однако, что такие телеустановки менее эффективны по сравнению с жестко ориентированными передающими телекамерами.

Отличительной особенностью некоторых объектов является их большая протяженность. Большое количество площадок таких объектов может быть расположено на значительном удалении друг от друга, что серьезно удорожает монтаж и эксплуатацию оборудования. В этих случаях можно применить систему малокадрового телевидения типа Slowscan. Она функционирует на больших дальностях, имеет невысокую стоимость и совместима с любой существующей замкнутой телевизионной системой, которая уже установлена на объекте. Для передачи видеокадров и команд в этой системе используется телефонная сеть общего пользования.

Особые преимущества в системах охраны имеют камеры на приборах с зарядовой связью (ПЗС). По сравнению с обычными трубочными камерами они обладают меньшими габаритами, более высокой надежностью, практически не нуждаются в техническом обслуживании, отлично работают в условиях низкой освещенности, обладают чувствительностью в инфракрасной области спектра. Однако, наиболее важным является то, что видеоинформация на чувствительном элементе указанной камеры сразу представлена в цифровой форме и без дополнительных преобразований пригодна для дальнейшей обработки. Это дает возможность легко идентифицировать различия или изменения элементов изображения, реализовать в камере встроенный датчик перемещений. Подобная камера со встроенным детектором и маломощным ИК – осветителем может вести наблюдение охраняемой территории и при появлении нарушителя в поле зрения распознавать изменения элементов изображения и подавать сигнал тревоги.

Несомненно, что в будущем появятся более миниатюрные и эффективные телекамеры, а по мере снижения стоимости расширится использование камер на ПЗС и формирователях видеосигналов. Прогресс в области видеосредств обнаружения перемещений, разрабатываемых в основном для военных целей, неизбежно приведет к появлению и на коммерческом рынке интеллектуальных камер, способных решать простые задачи распознавания.

По мере роста преступности все большее число предпринимателей начинают осознавать преимущества использования видеотехники в целях защиты собственности. Телевизионные системы могут применяться не только для внешней защиты объектов, но и для контроля действия персонала внутри объектов. Хорошим примером тому служит внедрение замкнутых телевизионных систем на автозаправочных станциях Великобритании. Такие системы позволяют идентифицировать нарушителей, получать вещественные доказательства вины мошенников, являются средством сдерживания потенциальных расхитителей.

3.4. Оборонительные системы

Для предотвращения развития вторжения на охраняемую территорию используется оборонительная система, в которой находят применение осветительные или звуковые установки. В обоих случаях субъект, пытающийся проникнуть на охраняемую территорию, информируется о том, что он обнаружен охраной. Таким образом, на него оказывается целенаправленное психологическое воздействие. Кроме того, использование осветительных установок обеспечивает благоприятные условия для действий охраны.

Для задержания преступника охрана предпринимает соответствующие оперативные меры или вызывает милицию (полицию). Если злоумышленнику удалось скрыться, то для успеха последующего расследования важное значение приобретает информация, которая может быть получена с помощью рассмотренной выше системы опознавания.

В особых случаях функции оборонительной системы выполняет специальное ограждение, через которое пропущен ток высокого напряжения.

3.5. Связная инфраструктура

Современный рынок технических средств предоставляет разработчикам широкие возможности выбора аппаратуры и каналов связи. Однако, с учетом интегрального подхода, в качестве связной инфраструктуры целесообразно использовать структурированные кабельные системы, такие как СКС Systimax компании Lucent Technologies. Требования к этим системам и их современные характеристики подробно описаны в Jet Info номер 16 за 1996 год.

3.6. Центральный пост и персонал охраны

Сложные комплексы защиты охраняемых территорий, состоящие, как правило, из нескольких систем, могут эффективно функционировать только при условии, что работа всех технических установок постоянно контролируется и управляется с центрального поста охраны. Учитывая повышенную психологическую нагрузку на дежурных охранников центрального поста, необходимость оперативной выработки и реализации оптимальных решений в случае тревоги, к центральным устройствам комплексов защиты предъявляются особые требования. Так, они должны обеспечивать автоматическую регистрацию и отображение всех поступающих в центральный пост сообщений и сигналов тревоги, выполнение всех необходимых процедур. Важную роль играет и уровень эргономики аппаратуры, которой оснащаются рабочие места дежурных охранников.

3.7. Интегральный комплекс физической защиты

На рис. 4 представлена блок-схема интегрального комплекса физической защиты объекта, обеспечивающего функционирование всех рассмотренных выше систем. Отличительной особенностью подобных комплексов является интеграция различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных.

Необходимо отметить, что в рассматриваемой блок-схеме технические средства скомпонованы по системам достаточно условно для того, чтобы схема приобрела более логичную форму и была бы более понятна. На самом деле одни и те же средства выполняют различные функции для разных систем обеспечения безопасности. В представленном виде блок-схема достаточно просто читается и дополнительного разъяснения не требует. Более подробно технические средства рассматриваются в следующих разделах.

4. Технические средства физической защиты

4.1. Средства контроля доступа

Мы переходим к рассмотрению средств обеспечения физической безопасности, которые используются при входе на охраняемый объект и/или внутри него.

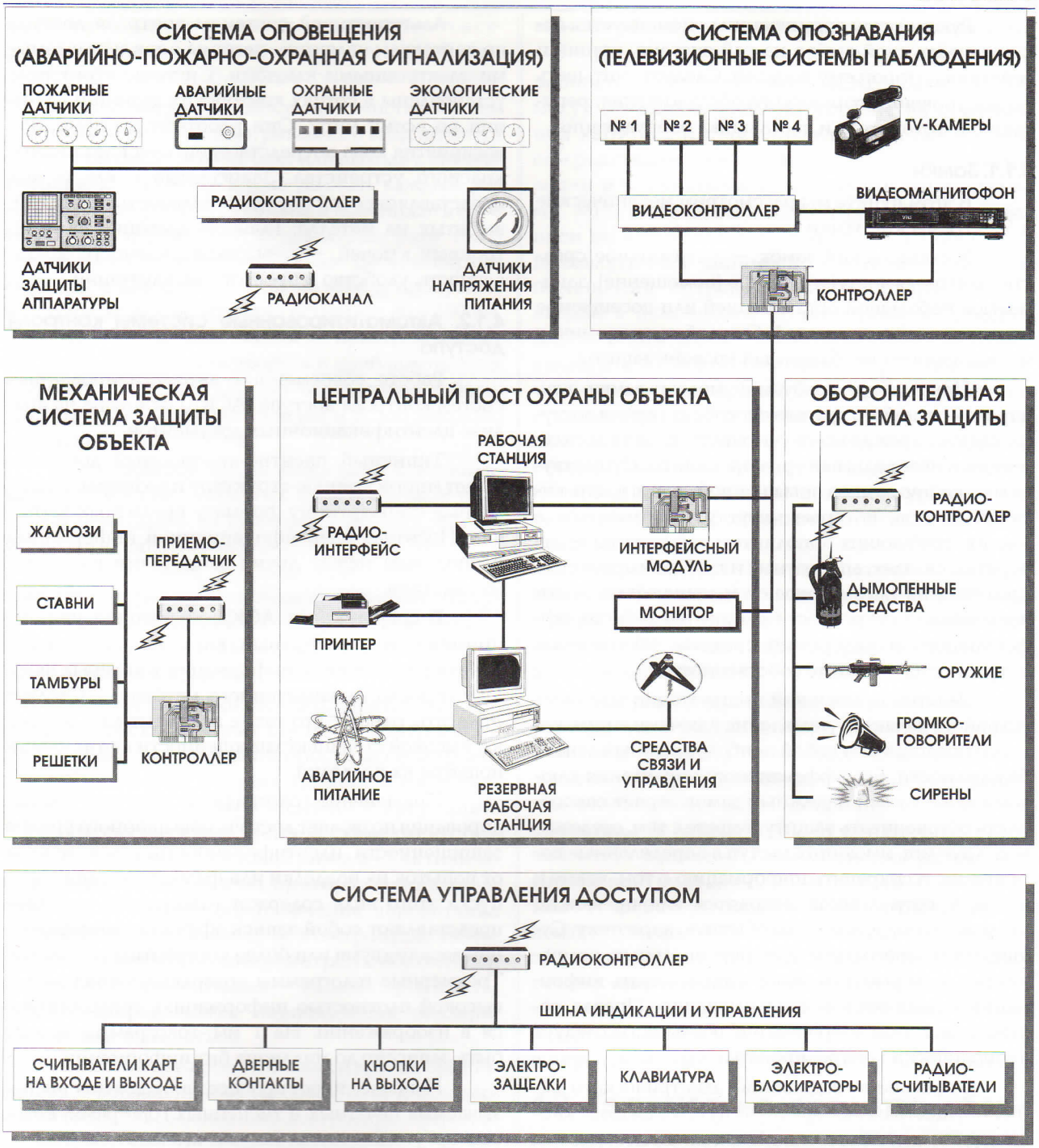

Рис. 4. Блок-схема интегрального комплекса физической защиты объекта.

При выборе системы контроля доступа рекомендуется проделать следующие действия:

- определить количество необходимых контрольно – пропускных пунктов, исходя из числа пропускаемых через них служащих, которых требуется проконтролировать с максимальной скоростью во время пиковой нагрузки;
- оценить требуемую степень безопасности организации. Ее можно повысить, к примеру, путем дополнения устройства считывания карточек средствами вводом персонального кода;
- предусмотреть средства аварийного выхода;
- оценить ассигнования, необходимые на приобретение, установку и эксплуатацию системы контроля доступа;

При выборе варианта системы, наряду с оценкой требуемого уровня безопасности и стоимости в сопоставлении с решаемыми задачами по контролю доступа, важно убедиться в том, что система достаточно проста в эксплуатации, обладает нужной гибкостью при изменении предъявляемых к ней требований, что ее можно наращивать, не теряя сделанных инвестиций. При выборе системы желательно заглянуть минимум на два года вперед.

Руководству организации рекомендуется останавливать свой выбор на той системе, принцип действия которой ему понятен. Следует учитывать также уровень технического обслуживания, репутацию изготовителя и поставщика оборудования.

4.1.1. Замки

В этом пункте мы рассмотрим механические и электрические замки.

Механический замок — оптимальное средство контроля доступа в здание (помещение), занимаемое небольшой организацией или посещаемое малым количеством людей. Он удобен, экономичен и обеспечивает необходимый уровень защиты.

При выборе требуемой модели замка, как, впрочем, и любого другого способа контроля доступа, следует прежде всего учитывать условия эксплуатации и необходимый уровень защиты. Существует множество замков повышенной секретности, висячих замков, которые могут устанавливаться в местах, требующих дополнительной защиты — на воротах, складах, аппаратных и т.д. Промышленные предприятия рассматривают механические замки повышенной секретности в качестве гибкого, эффективного и недорогого средства обеспечения потребностей в защите собственности.

Залогом правильной эксплуатации замковых устройств является управление ключами к ним, которое представляет собой наиболее важный аспект безопасности. Без эффективного управления ключами даже самый надежный замок теряет способность обеспечивать защиту. Вместе с тем, отслеживать круг лиц, имеющих доступ в определенные помещения, и сохранять информацию о том, какие и у каких сотрудников находятся ключи, можно столь же легко, как и вести обычную картотеку. Существуют программы для персональных компьютеров, которые позволяют поддерживать информацию о наличии ключей у служащих. Правда, соответствие этой информации реальности следует периодически контролировать.

Управление задвижкой электрического замка осуществляется вручную путем нажатия кнопок либо автоматически. Для отпирания двери с кнопочными замками (клавиатурой), требуется набрать правильный буквенно — цифровой код. Клавиатуру совместно с электрозамком обычно называют бесключевым средством контроля доступа. Недостатком кнопочных систем является возможность выявления кода путем подсматривания процесса его набора, анализа потертостей и загрязнений на кнопках и т.д.

В системах повышенной защищенности клавиатура может быть дополнена системой считывания карточек. Недостатком систем контроля доступа по карточкам является возможность утери последних, их хищения, передачи другому лицу.

Альтернативой системам контроля доступа по карточкам являются системы с так называемыми электронными ключами. Системы этого типа установлены в сотнях конторских зданий и гостиниц по всему миру. Они работают по принципу восприятия кода посредством оптического инфракрасного устройства. Записанный в ключе код представляет собой последовательность отверстий, выбитых на металле. Главные достоинства электронных ключей — невысокая стоимость, долговечность, удобство и простота эксплуатации.

4.1.2. Автоматизированные системы контроля доступа

Работа современных автоматизированных систем контроля доступа (АСКД) основана на анализе идентификационных документов.

Типичный идентификационный документ имеет многослойную структуру и размеры, аналогичные стандартному формату кредитных карточек. Носитель идентификационной информации расположен между двумя защитными пленками из пластика.

В современных АСКД достаточно широко применяются магнитные карточки, носителем идентификационной информации в которых является полоска намагниченного материала. Следует отметить, однако, что такие документы не обладают высокой степенью защищенности в отношении попыток их подделки.

Применение голографического способа кодирования позволяет достичь повышенного уровня защищенности идентификационных документов от попыток их подделки или фальсификации. Пропуска этого вида содержат голограммы, которые представляют собой запись эффекта интерференции между двумя или более когерентными полями. Трехмерные голограммы позволяют записывать с высокой плотностью информацию, содержащуюся в изображении. На 1 мм^2 голограммы может быть записано до миллиона бит информации.

Наиболее прост процесс изготовления так называемых печатных и тисненных голограмм, которые могут наноситься на уже имеющиеся идентификационные документы. Более сложна технология получения рефлексных голограмм, что и определяет обеспечиваемую ими повышенную степень защищенности документов от попыток подделки.

В последние годы заметно выросли масштабы применения в различных системах контроля доступа пропусков со встроенными интегральными схемами (ИС). Информация, хранящаяся в памяти карточки и/или вводимая пользователем, может обрабатываться микропроцессором карточки, устройством считывания или передаваться в центральную ЭВМ.

Использование пропусков с ИС позволяет проводить контроль доступа с высоким уровнем

надежности, однако стоимость таких документов существенно выше, чем карточек с магнитной полосой (1 — 2 доллара и 50 — 60 центов, соответственно).

Существенным недостатком многих систем контроля доступа рассматриваемого вида является то, что при проходе на объект или выходе с его территории владелец пропуска должен каждый раз вынимать документ из кармана и приближать его к устройству считывания. В последние годы были разработаны более совершенные бесконтактные системы, в которых расстояние между пропуском и устройством считывания составляет 40 — 100 см. При применении этих систем не приходится останавливаться, доставать пропуск и приближать его к устройству считывания, что обусловливает большие удобства для пользователей и более высокую пропускную способность.

В настоящее время выпускается несколько типов рассматриваемых бесконтактных систем. В некоторых из них кроме периферийных устройств считывания используется также и центральный блок, который выполняет основные процедуры по проверке правомочий доступа на охраняемый объект предъявителя пропуска и формирует сигналы управления механизмами блокировки прохода.

Идентификационные документы, используемые в бесконтактных системах контроля доступа, представляют собой пропуска со встроенной ИС. При этом находят применение как пассивные, так и активные носители информации. В первом случае в электронной схеме отсутствует собственный источник питания и ее активизация производится за счет преобразования энергии электромагнитного излучения передатчика устройства считывания. В электронной схеме активного носителя предусмотрен собственный источник электропитания — миниатюрная батарейка, которая может периодически подзаряжаться или заменяться.

В настоящее время в банках и других организациях с повышенными требованиями к безопасности находят все более широкое распространение биометрические системы контроля доступа, что можно объяснить снижением их стоимости.

В число биометрических систем контроля доступа входят системы проверки по форме кисти, ладони, рисунку кожи пальцев, сетчатке глаза, динамике подписи и по голосу. Все биометрические системы характеризуются высоким уровнем безопасности прежде всего потому, что используемые в них данные не могут быть утеряны пользователем, похищены или скопированы. В силу своего принципа действия биометрические системы отличаются малым быстродействием и низкой пропускной способностью. Тем не менее, они представляют собой единственное решение проблемы контроля доступа на особо важные объекты с малочисленным персоналом.

На крупных предприятиях возникает потребность в объединенных АСКД. Такие АСКД могут связывать воедино устройства считывания карточек и кнопочные устройства доступа со средствами пожарной и тревожной сигнализации и замкнутыми телевизионными системами. Многие АСКД позволяют распечатывать записи по каждому сигналу тревоги, а также осуществлять сбор данных по времени посещения помещений сотрудниками, по разрешенным входам в помещения, по попыткам несанкционированного входа, по полученным сигналам тревоги и их подтверждению. Подобные системы используются при высокой плотности потока проходящих лиц и большом числе устройств считывания с карточек. Будучи включенной в общую систему управления зданием, система контроля доступа может повысить уровень его защищенности. Основным достоинством объединенных систем является их гибкость, позволяющая руководству оперативно реализовывать решения по открытию или закрытию доступа в здания, помещения, лифты и целые этажи в установленное время зарегистрированным владельцам карточек.

На рис. 5 приведены сравнительные характеристики обеспечения безопасности современными электронными средствами контроля доступа, которые позволяют обеспечить решение необходимых задач по физической защите объектов. В зависимости от конкретных условий могут применяться комбинации различных систем контроля доступа, например, бесконтактные устройства считывания карточек при входе и выходе из здания в сочетании с системой контроля доступа по голосу в зоны обработки секретной информации. Наилучший выбор системы или сочетания систем может быть сделан только на основе четкого определения текущих и перспективных потребностей организации.

4.2. Технические средства обеспечения безопасности подвижных объектов

Среди достаточно широкой номенклатуры средств охраны подвижных объектов в последнее время наиболее активно развиваются автомобильные противоугонные системы. Стремление к высокой надежности, исключению ложных срабатываний, возможности скрытного размещения, оперативности формирования и доведения сигнала тревоги, определению местоположения мобильного средства определяют необходимость использовать при создании противоугонной аппаратуры эффективных технических решений, перспективных технологий и современной элементной базы.

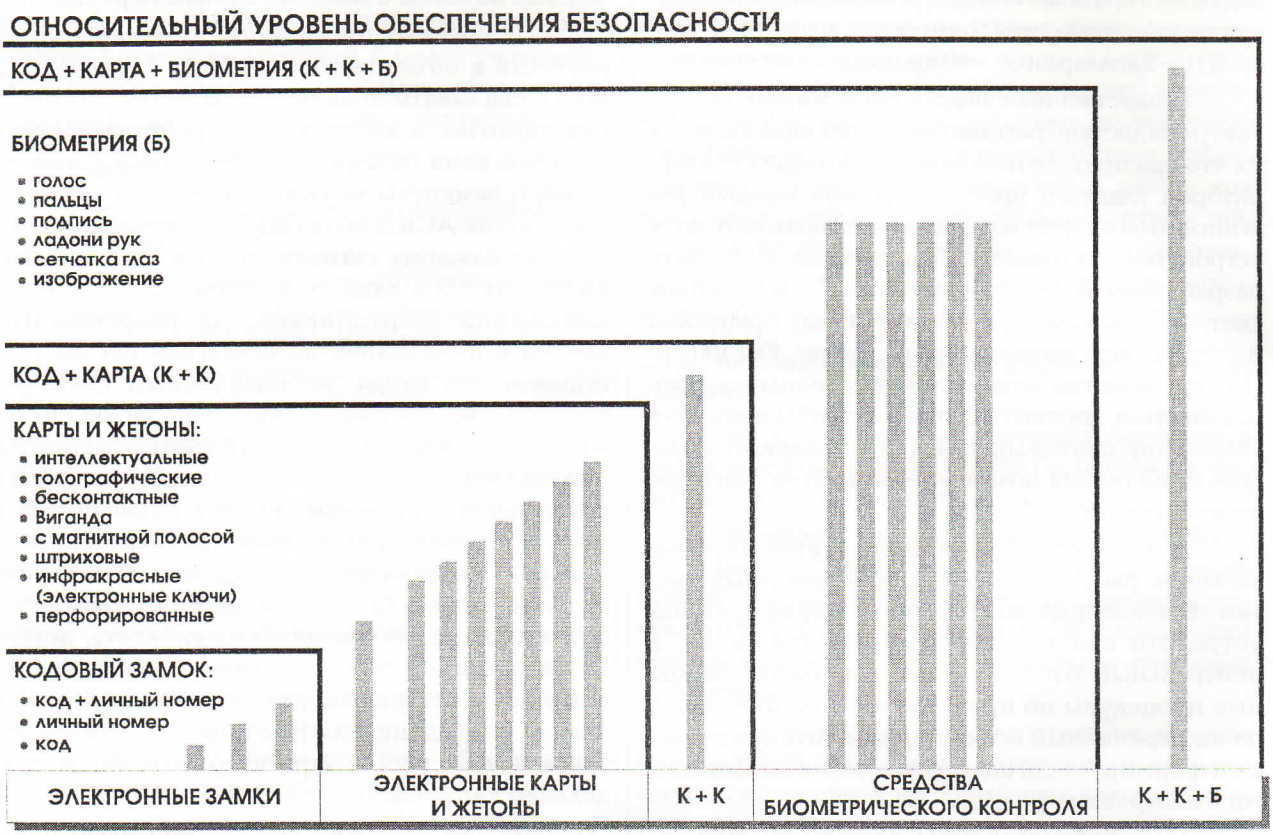

Рис. 5. Современные электронные средства контроля доступа.

Сердцем любой охранной системы являются датчики. В соответствии с ГОСТ 26342—84 наиболее часто в средствах обеспечения безопасности подвижных объектов используются следующие датчики:

- электроконтактные;
- магнитоконтактные;
- удароконтактные;
- электромагнитные бесконтактные;
- пьезоэлектрические;
- емкостные;
- ультразвуковые;
- вибрационные;
- оптико — электронные активные;
- оптико — электронные пассивные;
- оптико — электронные телевизионные;
- радиоволновые;
- акустические (звуковые).

Характеристики датчиков разных видов и рекомендуемые области их применения рассмотрены в Приложении.

Существующие технические средства охраны подвижных объектов можно классифицировать по следующим группам:

- механические устройства;
- отключающие и блокирующие приборы;
- электронные системы без дистанционного управления;
- электронные системы с дистанционным ключевым управлением.

Механические устройства выполняются в виде замков различной конфигурации со сложной (часто индивидуальной) формой ключа, скоб для блокирования органов управления (рулевая колонка, педали). Они обладают, как правило, высокой прочностью и требуют времени для устранения. В то же время, при наличии необходимого инструмента и благоприятствующей угонщику обстановки механические устройства охраны устраняются без труда.

Отключающие и блокирующие приборы, как правило, монтируются в системе подачи топлива или в цепи зажигания. Органы включения и выключения скрытно устанавливаются в салоне. Устройства просты, дешевы и удобны, но не исключают угон путем буксировки или погрузки на другое транспортное средство.

Типичное противоугонное устройство без дистанционного управления — это переносная установка, размещаемая снаружи автомобиля. При срабатывании охранного датчика включается дополнительная сирена с уровнем звукового сигнала более 110 дБ.

Абсолютное большинство современных электронных противоугонных систем строятся с использованием дистанционного управления по радиоканалу. Доступ в схему управления закрывается специальными кодовыми ключами. Отдель-

ные устройства имеют очень большое число вариантов кодирования (более 10 в степени 15), что исключает возможность вскрытия кодов даже при применении специальных сканирующих устройств. Формирование команд управления и их ретрансляция в радиоканал осуществляется с помощью маломощных миниатюрных передатчиков, а прием, декодирование и выделение сигналов, воздействующих на исполнительные устройства — с помощью миниатюрных приемников, скрытно размещаемых в автомобиле. В качестве исполнительных устройств могут использоваться электрические замки, бортовая световая и звуковая сигнализация, система защиты двигателя. Для других систем характерно включение дополнительных сирен с уровнем звука 110 — 130 дБ, которые, сигнализируя о несанкционированном проникновении в автомобиль, оказывают ощутимое воздействие на слух угонщика, находящегося в салоне.

Для индивидуального оповещения пользователей применяются звуковые и визуальные сигнализаторы, встраиваемые в носимые приемные устройства (пьезокерамические элементы, жидкокристаллические дисплеи).

Существующие средства защиты подвижных объектов могут быть весьма эффективно использованы и для защиты стационарных объектов в нестандартных ситуациях (например, при временном развертывании технических средств и систем).

4.3. Технические средства охранной сигнализации физических лиц

Как правило, современные системы охранной сигнализации физических лиц строятся на основе специализированных средств радиосвязи. Приемник системы устанавливается в дежурном помещении, либо мобильном пункте центра охраны; передатчик, скрытый в верхней одежде физического лица, автоматически формирует сигнал тревоги в критических ситуациях. В число таких ситуаций обычно входит:

- несанкционированная попытка выключения передатчика;
- удаление передатчика из зоны уверенного приема системы;
- нажатие специальной клавиши тревоги;
- неподвижность физического лица в течение заданного интервала времени;
- критический угол наклона передатчика, фиксирующий горизонтальное положение охраняемого лица.

В некоторых системах передатчик оснащается датчиком, контролирующим физиологические параметры охраняемого лица: глубину дыхания, частоту пульса, уровень кровяного давления. Это позволяет формировать сигнал тревоги при резких изменениях перечисленных показателей.

Рассматриваемые системы применяются для обеспечения безопасности физических лиц в соответствии с договорами, а также как эффективное средство контроля за собственной безопасностью сотрудников охранных подразделений, выполняющих задания в опасных для здоровья или жизни условиях.

Для повышения эффективности управления подразделениями охраны внутри охраняемого объекта могут использоваться системы определения местоположения сотрудников на основе активных инфракрасных меток.

Большими возможностями обеспечения безопасности обладают пейджинговые системы, которые состоят из центрального пульта управления, передатчика с антенной и ряда индивидуальных абонентских устройств (пейджеров), принимающих и отображающих переданную информацию.

Подобные системы персонального радиопоиска (СПР) особенно эффективны в условиях ограниченной территории, когда мобильная связь экономически не оправдана. Высокая экономическая эффективность СПР достигается за счет резкого ограничения необходимого для связи спектра частот (путем односторонней передачи узкополосных двоичных сигналов от всех абонентов на одной радиочастоте) и за счет значительного уплотнения передаваемых сигналов во времени (путем последовательной пакетной передачи накопленной информации от каждого абонента). Основным недостатком подобных систем является то, что абонент может только принимать информацию, а передавать ее не может.

Особый интерес для систем физической безопасности представляют так называемые альтернативные пейджинговые системы, в которых приемник и передатчик меняются местами. В этом случае решается обратная задача: передача сигналов тревоги от абонента, идентификация и определение местоположения источников сигналов тревоги, поэтому каждый абонент имеет пейджер — передатчик, передающий заготовленную заранее тревожную информацию на общий для всех абонентов сети приемник, на котором осуществляется прием и обработка тревожных сигналов.

Данная система является в настоящее время, пожалуй, наиболее гибким и экономически выгодным средством приема сигналов тревоги, обеспечивающим эффективную реакцию в критических ситуациях и позволяющим ответить на три основных вопроса: кто? где? когда? Она идентифицирует кто включил сигнал тревоги, где и когда это произошло. Кроме того, имеется возможность направить информацию о происшествии не только на стационарные пункты службы безопасности, но и на портативные карманные пейджеры персонала, находящегося в пути.

5. Заключение

Как показывают результаты проведенного анализа, методы и технические средства обеспечения физической безопасности получили в настоящее время новый импульс в своем развитии, в частности:

- возник новый класс технических средств телеобслуживания, в который, помимо традиционного охранного телевидения, вошли технические средства тепловизионного, лазерного, радиотехнического, ночного видения и др.;
- средства контроля доступа поднялись на качественно новую ступень благодаря использованию биометрических и криптографических методов идентификации;
- появились принципиально новые возможности в системах персональной охранной сигнализации физических лиц (с одновременным приемом сигналов тревоги стало возможным определение местоположения физических лиц);
- тенденция интеграции захватила и технику обеспечения физической безопасности.

Являясь неотъемлемой частью информационной безопасности, средства физической защиты и сегодня играют очень важную роль в обеспечении интегральной информационной безопасности. При отсутствии надежной физической защиты становятся неэффективными практически все известные меры обеспечения безопасности. Поэтому, методы и технические средства физической защиты требуют к себе постоянного внимания, их необходимо изучать и совершенствовать.

6. Приложение

Датчики тревожной сигнализации для систем обеспечения физической безопасности

При конструировании системы защиты одной из центральных задач является выбор оптимальных средств оповещения и, в первую очередь, датчиков тревожной сигнализации. В настоящее время разработано и используется большое количество самых разнообразных датчиков сигнализации. Рассмотрим кратко принципы действия, отличительные особенности и способы применения наиболее распространенных из них.

Периметральные датчики натяжного действия

Датчики этого типа состоят из нескольких рядов натянутой проволоки, подсоединенной к механическим выключателям. Малейший изгиб проволоки вызывает срабатывание сигнализации.

Для монтажа датчиков натяжного действия используется, как правило, колючая проволока. Выключатели устанавливаются на специальных стойках, которые отстоят друг от друга на 60 см.

Проволока натягивается с усилием до 45 кг, механизм выключателя срабатывает при изгибе проволоки свыше 2 мм. Преодоление таких датчиков возможно за счет перелезания по датчиковым стойкам.

Периметральные инфраакустические датчики

Устанавливаются на металлических ограждениях и улавливают низкочастотные звуковые колебания ограждений во время их преодоления. Возможны ложные срабатывания таких датчиков на уличные шумы от близко расположенных дорог.

Периметральные датчики электрического поля

Датчики этого типа состоят из двух частей: излучателя и нескольких приемников. Обе части датчика выполнены из электрических кабелей, натянутых между столбами. Во время прохождения нарушителя между излучателем и приемниками имеет место изменение электрического поля между ними, которое и является сигналом тревоги.

Периметральные вибрационные датчики

Датчики этого типа представляют собой контактные выключатели различных видов, соединенные последовательно или параллельно. Датчики крепятся на столбах или сетках ограждений и срабатывают от качаний, сотрясений или вибраций. Такие датчики оборудуются, как правило, микропроцессорами для обработки сигналов от контактных выключателей и формирований и посылки команды тревоги на центральный пост охраны.

Контактные выключатели вибрационных датчиков по принципу действия бывают ртутными, шариковыми, пьезоэлектрическими и маятниковыми.

Периметральные электретные датчики

Изготавливаются из коаксиального кабеля с радиально поляризованным диэлектриком. Такой кабель протягивается через ограждения периметра объекта. В момент преодоления ограждения происходит сотрясение кабеля и, соответственно, изменение электрического сигнала, проходящего через кабель.

Как и вибрационные, электретные датчики оснащаются микропроцессорами для контроля порогового уровня срабатывания и могут быть отрегулированы на распознавание воздействий, вызываемых ветром, брошенными камнями или другими предметами, животными, птицами, вибрации почвы от движущихся транспортных средств, градом или снегом, землетрясением, движением веток деревьев.

Периметральные вибрационные и электретные датчики могут обходиться путем подкопа или преодоления сверху без их касания.

Инфракрасные датчики контроля пространства

Принцип действия датчиков основан на изменении сигнала от излучателя к приемнику при попадании нарушителя между ними.

В качестве излучателей используются инфракрасные светодиоды или небольшие лазерные установки. Расстояние между излучателем и приемником не более 100 метров. На специальные столбы обычно устанавливают несколько таких устройств для создания вертикальной полосы обнаружения необходимой высоты. Для повышения надежности иногда используется частотная модуляция сигнала излучения.

Датчики могут терять свою работоспособность при густом тумане и снегопаде.

Микроволновые датчики контроля пространства

Состоят из двух частей: сверхвысокочастотных передатчика и приемника, которые устанавливаются на расстоянии до 150 метров друг от друга. В этом пространстве между ними создается электромагнитное поле, изменение которого при попытке прохода регистрируется приемником. Для эффективной работы таких датчиков необходимо, чтобы высота неровностей почвы не превышала 5 — 7 см, а в зоне действия не было растительности.

Сейсмические датчики

В настоящее время изготавливается два вида датчиков этого типа. Первый, жидкостной, состоит из двух уложенных рядом в почву шлангов с жидкостью. Срабатывание таких датчиков происходит при изменении давления в одном из шлангов при прохождении нарушителя.

Принцип действия датчиков второго вида основан на пьезоэлектрическом эффекте, при котором происходит изменение электрического сигнала при давлении на пьезоэлемент.

Оба вида сейсмических датчиков чувствительны к посторонним вибрациям, вызываемым, например, проезжающим транспортом или сильным ветром.

Сейсмические датчики используются для охраны периметров территорий и зданий, устанавливаются скрытно в почву или ее покрытие, под поверхности стен и строительных конструкций.

Магнитные датчики

Изготавливаются из проволочной сетки, которая укладывается в почву. Датчики этого типа реагируют на прохождение человека с металлическим предметом достаточно большой массы. Наличие металла вызывает индукционные изменения электрического поля проволочной сетки, что и возбуждает сигнал тревоги.

Магнитные датчики неэффективные вблизи автомобильных и железных дорог. Возможны ложные срабатывания от грозовых разрядов, мощных электромоторов и реле.

Сейсмомагнитные датчики

Выполняются в виде электрического кабеля, уложенного в почву. Электрический сигнал изменяется под воздействием как сейсмических, так и магнитных возмущений, например, при проходе человека и проносе им оружия. Причины ложных срабатываний те же, что и в предыдущем случае.

Электромеханические выключатели

Действие датчиков этого типа основано на регистрации разрыва электрической цепи при воздействии нарушителя. Они применяются для контроля периметров зданий и помещений. Изготавливается два вида датчиков: как с неразрушающимися элементами (типа кнопок), так и с разрушающимися контактами при использовании, например, токопроводящего стекла или сетки из фольги.

Магнитные выключатели

Датчики этого типа состоят из выключателя (так называемого геркона), контакты которого размыкаются или замыкаются под воздействием магнита. Датчик состоит из двух частей: подвижной и неподвижной. На подвижной части, например, двери или оконной раме устанавливается магнит, а на неподвижной — геркон, который при открывании подвижной части размыкает электрическую цепь и вызывает появление сигнала тревоги.

Проволочные сетки

Используются для обнаружения проникновения в помещение через стены, полы, потолки, двери, окна и другие конструкции. Охраняемая поверхность покрывается сеткой из электрического провода с размерами ячеек 10 — 15 см. Механическое разрушение ячеек сетки приводит к разрыву проводников и, соответственно, к разрыву электрической цепи.

Для маскировки сетка датчика может покрываться обоями или облицовочными материалами.

Ультразвуковые датчики

Действие основано на регистрации ультразвуковых волн от нарушителя при его воздействии на элементы конструкций периметра здания или помещения. Используются как пассивные, так и активные ультразвуковые датчики.

Пассивные регистрируют ультразвуковые колебания воздуха или другой среды на частотах 18 — 60 кГц, возникающие при попытке разрушения металлических конструкций механическим или термическим способом.

Выпускается две разновидности активных ультразвуковых датчиков. В первой используются элементы конструкций периметра охраняемых по-

мещений. При таком воздействии как, например, разбивание оконного стекла, нарушается связь передатчика и приемника через стекло и происходит срабатывание датчика.

Активные ультразвуковые датчики второго вида регистрируют изменение частоты (излучаемого датчиком сигнала) в охраняемой среде, например, при открывании замка или отпиливании металлической решетки.

Емкостные датчики

Датчики этого типа применяются для охраны защитных металлических решеток инженерных коммуникаций. Действие датчиков основано на регистрации изменения электрической емкости между полом помещения и решетчатым внутренним ограждением.

Ультразвуковые датчики для контроля помещений

Датчики этого типа с излучающей и приемной частями регистрируют изменение сигнала излучения, отраженного от нарушителя.

Для помещений площадью до 50 м^2 могут применяться однокорпусные датчики. Большие по размерам помещения охраняются двухкорпусными датчиками: излучатель в отдельном корпусе крепится на одной стене, а приемник (или несколько приемников) — на противоположной стене.

Находящиеся в помещении крупногабаритные предметы ограничивают действие такого датчика, создавая области экранировки ("мертвые зоны"), в которых датчик не реагирует на движение нарушителя.

Микроволновые датчики

Работают в СВЧ—диапазоне на частотах порядка 10.5 ГГц. Излучение и прием осуществляется одной антенной.

Фотоэлектрические датчики

Работа этого вида датчиков основана на прерывании нарушителем луча света любого диапазона, сформированного соответствующим фильтром.

Акустические датчики

В состав этих датчиков входят микрофон и блок обработки сигналов. Они служат для обнаружения вторжений преступников и реагируют на шум и звуки, которые неизбежно возникают при попытке проникнуть в охраняемое помещение.

Барометрические датчики

Весьма перспективный тип датчиков, который активно используется в последнее время в системах охранной сигнализации. Предназначен для охраны закрытых объемов помещений. Датчик реагирует на флуктуации давления воздуха в охраняемом помещении. Устойчив к воздействию шумов, вибрации, перемещению людей и животных, не оказывает вредного влияния. Срабатывает в момент открывания дверей, окон, форточек или при разрушении стен, потолка, дверей и окон. Очень экономичен (ток потребления — не более 1 мА).

Конференция
Со стр 2

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ N 1806-р

от 7 декабря 1996 г.

г.Москва

1. Согласиться с предложением Гостехкомиссии России о проведении в г.Москве с 14 по 18 апреля 1997 г. международной конференции «Безопасность информации» и тематической выставки.
2. Утвердить Заместителя Председателя Правительства Российской Федерации Лобова О.И. председателем оргкомитета международной конференции «Безопасность информации».

   Лобову О.И. утвердить состав оргкомитета.
3. Федеральным органам исполнительной власти и органам исполнительной власти субъектов Российской Федерации оказать необходимую помощь оргкомитету в подготовке и проведении международной конференции «Безопасность информации» и тематической выставки.
4. В целях обеспечения финансирования подготовки и проведения международной конференции «Безопасность информации» и тематической выставки разрешить оргкомитету привлекать внебюджетные источники финансирования.

Председатель Правительства Российской Федерации *В. Черномырдин*

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается компанией Инфосистемы Джет с 1995 года
Подписной индекс 32555

Главный редактор: Галатенко В.А. *(galat@jet.msk.su)*
Технический редактор: Демочкин С.И. *(serged@jet.msk.su)*

Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
e-mail: JetInfo@jet.msk.su