**1. Техническая укрепленность периметра защищаемого объекта**

Характерной тенденцией развития информационных технологий является процесс 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).

Задача обеспечения информационной 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 (способных 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;
* 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 рисунке 4.1 представлены технические средства противодействия и соответствующие подсистемы, имеющиеся в распоряжении разработчика.

|  |
| --- |
| graphics  Рисунок 4.1. - Структура объединенной системы обеспечения безопасности |

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 рисунке 4.2 этот процесс представлен в графической форме.

|  |
| --- |
| graphics  Рисунок 4.2. - Процесс выбора средств противодействия |

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 рисунке 4.2). 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. Рисунок 4.3 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.

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.

|  |
| --- |
| graphics  Рисунок 4.3. - 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. |

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.

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).

# Механические системы защиты

Основой любой механической системы зашиты, 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.

# 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 маскировочного 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.

# 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 выше сформулированного 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.

# 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.

# 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.

# 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.

# Интегральный комплекс физической защиты

На рисунке 4.4 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.

|  |
| --- |
| graphics  Рисунок 4.4. - Блок-схема интегрального комплекса физической защиты объекта |