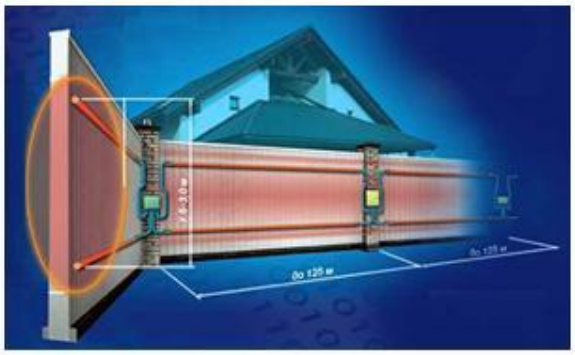
Организация инженерной системы защиты объектов



Организация систем защиты - это комплекс организационных и технических мероприятий направленных на обнаружение, отражение и ликвидацию различных видов угроз объекту.
Прежде чем переходить к изложению основного материала во избежание различных толкований необходимо на основании действующих нормативов определить основные термины, используемые в различных системах безопасности.

Комплекс охранно-пожарной сигнализации – это совокупность совместно действующих технических средств охранной, пожарной и/или охранно-пожарной сигнализации, установленных на охраняемом объекте и объединенных системой инженерных сетей и коммуникаций.
Охранная сигнализация - получение, обработка, передача и представление в заданном виде при помощи технических средств потребителям информации о проникновении на охраняемые объекты.
Охранно-пожарная сигнализация - получение, обработка, передача и представление в заданном виде при помощи технических средств потребителям информации о проникновении на охраняемые объекты и о пожаре на них.
Охраняемый объект - объект, охраняемый подразделением охраны и оборудованный действующими техническими средствами охранной, пожарной и/или охранно-пожарной сигнализации.
Охраняемая зона - часть охраняемого объекта, контролируемая одним шлейфом охранной сигнализации (для комплексов охранной сигнализации), одним шлейфом пожарной сигнализации (для установок пожарной сигнализации), одним шлейфом охранно-пожарной сигнализации (для комплексов охранно-пожарной сигнализации).
Пульт централизованного наблюдения - самостоятельное техническое средство (совокупность технических средств) или составная часть системы передачи извещений, установленная в пункте централизованной охраны для приема от оконечных устройств или ретрансляторов извещений о проникновении на охраняемые объекты и/или пожаре на них, служебных и контрольно-диагностических извещений, обработки, отображения, регистрации полученной информации и представления ее в заданном виде для дальнейшей обработки, а также {при наличии обратного канала) для передачи через пультовое оконечное устройство на ретранслятор) и объектовые оконечные устройства команд управления.
Шлейф охранной (пожарной, охранно-пожарной) сигнализации - электрическая цепь, соединяющая выходные цепи охранных (пожарных, охранно-пожарных) извещателей, включающая в себя вспомогательные (выносные) элементы (диоды, резисторы и т.п.) и соединительные провода и предназначенная для выдачи на приемно-контрольный прибор извещений о проникновении (попытке проникновения) пожаре и неисправности, а в некоторых случаях и для подачи электропитания на извещатели.
Автоматическая система тревожной сигнализации - Система тревожной сигнализации (система охранной, охранно-пожарной сигнализации) обеспечивающая автоматический переход из нормального состояния в отключенное и обратно под управлением ответственного лица и\или владельца без обращения к другим системам, например, к системе связи.

Прим. данная статья взята с сайта http://os-info.ru

Защита от попыток несанкционированного доступа - применение электрических или механических средств для предупреждения несанкционированного доступа в систему или ее часть.
Защищенность объекта - совокупность организационно-технических мероприятий, направленных на обеспечение охраны объекта (зоны объекта).
Инженерно-техническая укрепленность охраняемого объекта - совокупность мероприятий, направленных на усиление конструктивных элементов зданий и помещений, а также ограждений объекта для предотвращения проникновения в охраняемую зону.
Категория охраняемого объекта - комплексная оценка состояния объекта, учитывающая его экономическую или иную (например, культурную) значимость в зависимости от характера и концентрации сосредоточенных ценностей, последствий от возможного преступного посягательства на них, сложности обеспечения требуемой надежности охраны.
Ложная тревога - извещение о тревоге, формируемое в результате ошибок вызванных следующими причинами:
- случайным нажатием ручного вызывного устройства (кнопки тревоги); реагированием автоматического устройства на состояние, которое оно не должно обнаруживать;
- дефектом или отказом элементов системы; ошибочными действиями оператора (пользователя).
Многорубежный комплекс охранной сигнализации - совокупность двух и более рубежей охранной сигнализации, в каждом из которых применяются технические средства охранной сигнализации, основанные на разных физических принципах действия.
Нарушитель - лицо, пытающееся проникнуть или проникшее в помещение (на территорию), защищенное системой охранной или охранно-пожарной сигнализации без разрешения ответственного лица, пользователя, владельца.
Охраняемая зона - часть здания и/или территории (объекта), в которой может (должна) быть обнаружена опасность с помощью системы тревожной сигнализации.
Пункт централизованной охраны - диспетчерский пункт для централизованной охраны ряда рассредоточенных объектов от проникновения нарушителя и пожара с использованием систем передачи извещений о проникновении и пожаре.
Рубеж охранной сигнализации - совокупность совместно действующих технических средств охранной сигнализации, последовательно объединенных электрической цепью, позволяющей выдать извещение о проникновении (попытке проникновения) в охраняемую зону (зоны) независимо от других технических средств, не входящих в данную цепь.
Система охранной сигнализации - 1) совокупность совместно действующих технических средств обнаружения проникновения (попытки проникновения) на охраняемый объект сбора, обработки, передачи и представления в заданном виде потребителю информации о проникновении (попытке проникновения) и другой информации;
2) совокупность совместно действующих технических средств для обнаружения появления признаков нарушителя на охраняемом объекте, передачи, сбора, обработки и представления информации в заданном виде.
Система охранно-пожарной сигнализации - совокупность совместно действующих технических средств для обнаружения появления признаков нарушителя на охраняемых объектах и/или пожара на них, передачи, сбора, обработки и представления информации в заданном виде.
Состояние тревоги - состояние системы тревожной сигнализации или ее части, являющееся результатом реагирования системы на наличие опасности, при котором она выдает извещение о тревоге.
Состояние контроля - состояние системы тревожной сигнализации, при котором обеспечивается проверка ее функционирования.
Степень риска - вероятностная величина, характеризующая возможность невыполнения системой или комплексом своей целевой задачи (обнаружение проникновения или попытки проникновения на охраняемый объект) с учетом влияния опасных внутренних и внешних воздействий на функционирующие систему или комплекс.
Тактика охраны объекта - выбор вида охраны, методов и средств его реализации.
Техническое средство охранной сигнализации - конструктивно законченное, выполняющее самостоятельные функции (аппаратно-программное) устройство, входящее в состав системы, комплекса охранной сигнализации.

Тревога - предупреждение о наличии опасности либо угрозы для жизни, имущества или окружающей среды.
Уровень риска - показатель, характеризующий величину опасности для людей и имущества в окружающей их среде.
Уровень защиты - показатель, характеризующий результат влияния технических и организационных мер, предпринимаемых для обеспечения безопасности и сохранности людей и имущества.
Уровень безопасности - показатель, характеризующий превышение уровнем защиты уровня риска.
Устройство защиты от несанкционированного *доступа* - устройство предназначенное для обнаружения несанкционированного доступа к элементу или составной части системы тревожной сигнализации.
Шлейф охранной сигнализации - электрическая цепь, соединяющая выходные цепи охранных извещателей, включающая в себя вспомогательные элементы и соединительные провода и предназначенная для передачи на приемно-контрольный прибор извещений о проникновении и неисправности, а в некоторых случаях и для подачи электропитания на охранные извещатели.
Инженерно-технические мероприятия по усилению охраны - охранное телевидение и освещение, постовая сигнализация и связь, места и оборудование для контроля прохода и досмотра, контрольно-следовые полосы, ограждения, запрещающие, предупреждающие, указательные и разграничительные знаки и т.п.
Инженерно-техническая укрепленность - совокупность мероприятий, направленных на усиление конструктивных элементов зданий и помещений, а также ограждений объектов для предотвращения проникновения в охраняемую зону.
Рубеж охранной сигнализации - совокупность технических средств охранной сигнализации, позволяющих выдавать извещения о проникновении на отдельный номер приемно-контрольного прибора или пульта централизованного наблюдения, размещаемых в пунктах централизованной охраны или дежурных частях, независимо от наличия других рубежей охраны на объекте.
Тревожная сигнализация - совокупность технических средств, позволяющая выдавать сигналы тревоги в дежурные части ОВД при разбойном нападении на объект в период его работы или при визуальном обнаружении нарушений системы охраны объекта.
Вероятность ложного срабатывания - математическая величина возможности срабатывания при отсутствии пожара на охраняемом объекте, проникновении (попытке проникновения) нарушителя или неисправности технических средств.
Извещение - сообщение, несущее информацию о проникновении (попытке проникновения, физическом воздействии, превышающем нормированный уровень на зону обнаружения извещателя или его чувствительный элемент) на охраняемом объекте и передаваемое с помощью электромагнитных, электрических, световых и/или звуковых сигналов.
Ложные тревоги -
1) выдача тревожного сообщения о пожаре, проникновении или неисправности без наличия пожара на объекте, проникновения (попытки проникновения), неисправности технического средства;
2) извещение о тревоге, формируемое в результате ошибки, вызванной следующими причинами:
- случайным нажатием ручного вызывного устройства (кнопки); реагированием автоматического устройства на состояние, которое оно не должно обнаруживать;
- дефектом или отказом элементов системы;
- ошибочными действиями оператора (пользователя).
Ложное срабатывание технического средства - изменение, вызванное техническим средством при отсутствии контролируемых изменений состояния охраняемого объекта или технического средства. Помехозащищенность -числовое значение основного параметра источника помехи, до достижения которого техническое средство охранной, пожарной или охранно-пожарной сигнализации не должно выдавать ложное срабатывание.
Средний период ложных срабатываний - нижняя граница статистической оценки среднего периода следования одиночных ложных срабатываний технического средства в стандартных условиях испытаний, установленных в стандартах или технических условиях.

Автоматический пожарный извещатель - пожарный извещатель, реагирующий на факторы, сопутствующие пожару.
Дымовой пожарный извещатель - автоматический пожарный извещатель, реагирующий на аэрозольные продукты горения.
Пожарный извещатель - устройство для формирования сигнала о пожаре.
Пожарный оповещатель - устройство для массового оповещения людей о пожаре.
Ручной пожарный извещатель - пожарный извещатель с ручным способом приведения в действие.
Тепловой пожарный извещатель - автоматический пожарный извещатель, реагирующий на определенное значение температуры и/или скорости ее нарастания.
Установка пожаротушения - совокупность стационарных технических средств для тушения пожара за счет выпуска огнетушащего состава.
Установка пожарной сигнализации - совокупность технических средств, установленных на защищаемом объекте, для обнаружения пожара, обработки, представления в заданном виде извещения о пожаре на этом объекте, специальной информации и/или выдачи команд на включение автоматических установок пожаротушения и технические устройств.

Общие положения

Для осуществления действенного управления, предотвращения материальных потерь от несанкционированных действий злоумышленников необходимо выполнение требований, изложенных в концепции организации безопасности конкретного объекта.
Концепция безопасности - система взглядов по обеспечению безопасности объекта от прогнозируемых угроз.

Одной из главных задач руководителей предприятий является обеспечение стабильной деятельности своих производственных объектов. Стабильная работа любого предприятия невозможна без надежной защиты от действий, убытки от которых могут быть весьма существенны. При организации и обеспечении защиты предприятий следует учитывать комплексный характер организационно-технических мероприятий по обеспечению безопасности. Если в системе безопасности хотя бы один из компонентов будет иметь изъяны, остальные ее составляющие не смогут в нужный момент противостоять угрозам, даже в случае значительного усиления их защитных свойств.

Безопасность объекта физическая - состояние защищенности жизненно-важных интересов (объекта) от угроз, источниками которых являются умышленные противоправные (несанкционированные) действия физических лиц (нарушителей).

Защита каждого объекта, а также подходы к ее реализации строго индивидуальны. Пути построения защиты в значительной мере зависят от того, в каком состоянии находится объект: в стадии проектирования, строительства или эксплуатации, какие площади он занимает, какие материальные ценности там сосредоточены и т.п. вопросы. Этапы работ по оснащению объектов системами безопасности приведены в **Приложении 1.** Целесообразнее всего закладывать основы защиты на этапе проектирования, с учетом всех характерных для объекта особенностей. К сожалению, приходится констатировать, что об этом вспоминают тогда, когда на объекте уже закончены отделочные работы и в связи с этим Заказчик выдвигает дополнительные требования, которые, как правило, ведут к удорожанию работ
Организация системы защиты - это комплекс организационных и технических мероприятий направленных на обнаружение, отражение и ликвидацию различных видов угроз объекту.

Система защиты (СЗ) представляет собой совокупность организационно - правовых и инженерно-технических решений, направленных на защиту интересов и ресурсов предприятия (объекта) от угроз, источниками которых являются злоумышленные действия нарушителей.
Оптимальная система защиты позволяет сократить расходы на содержание штата службы безопасности и, в тоже время, повысить эффективность обеспечения безопасности объекта в целом. При использовании такой системы нет необходимости в организации постоянной постовой службы по периметру объекта; вместо этого создаются дежурные тревожные группы, которые предпринимают немедленные действия по нейтрализации нарушителей после получения сигнала тревоги на центральном пульте управления или на посту охраны. Информация о факте нарушения документируется в компьютерной базе данных с фиксацией времени и зоны нарушения. В разработанной таким образом системе влияние человеческого фактора сводится до минимума и достигается высокая эффективность защиты объекта при минимальном количестве личного состава сил охраны.

Эффективность системы защиты - вероятность выполнения системой своей основной целевой функции по обеспечению защиты объекта от угроз, источниками которых являются умышленные противоправные (несанкционированные) действия физических лиц (нарушителей).
Учитывая сложность решаемых задач, исходя из принципов рационального и эффективного использования денежных средств, создание системы защиты должно базироваться на:
- разумной достаточности мер;
- четкой правовой основе;
- организованной службе физической охраны;
- оптимальном составе технических средств защиты.

Реализация этих принципов требует комплексного подхода при проектировании и внедрении системы безопасности объектов.

Основными задачами СЗ являются: обнаружение, отражение и ликвидация угроз.

К средствам **обнаружения** и **отражения** относятся, как правило, технические системы, т.е. системы охранно-пожарной сигнализации, телевизионного наблюдения, а также инженерно-технические средства в виде ограждения объекта, усиленных дверей и стен, т.е. средств преграждающих и отражающих несанкционированное проникновение на территорию и в помещения.

К средствам **ликвидации** угроз относится служба физической охраны объекта (служба безопасности), в задачи которой входит задержание и обезвреживание злоумышленника. Аналогичные функции решают некоторые технические средства (система автоматического пожаротушения, система автоматического блокирования отдельных зон и т.п.)

При оценке уровня безопасности объекта и последующим созданием системы защиты необходимо предварительно провести анализ возможных угроз, оценить вероятность их появления, а затем выбрать адекватные средства и методы защиты. Категории объектов, их состав и системы, рекомендуемые для их защиты, приведены в **Приложении 2.**

При определении экономической эффективности систем технической безопасности следует рассматривать соотношение стоимости возможного предотвращаемого ущерба (от пожара, кражи и т.п.) к прямым затратам на их внедрение и эксплуатационно-техническое обслуживание. Даже самое простое сравнение ущерба от кражи и от пожара показывает, что кроме чисто материального ущерба при пожаре возможна еще и гибель людей. Кроме того, значительные средства затрачиваются впоследствии на восстановление строительной части объектов. Величина ущерба складывается из:
- стоимости, направленной на возмещение последствий события (компенсация);
- стоимости похищенного или уничтоженного пожаром имущества, ремонт объекта и т.п.);
- стоимости дополнительных временных расходов (восстановление работоспособности участка, которому нанесен ущерб);
- относительной стоимости, определенной убытками из-за случившегося хищения или пожара (простоя оборудования, штрафами за срыв сроков поставки и т.п.);
- размера затрат и рабочего времени, потраченных на расследование происшествий.

Перечисленные виды стоимости образуют так называемую "группу риска". Разница между возможными потерями и прямыми затратами составит условную прибыль по конкретной системе. Величина этой условной прибыли определяет величину капиталовложений в оборудование объекта техническими средствами, различных систем безопасности.

При возникновении сомнений в выборе аппаратуры надо ответить на вопросы:
- какие причины лежат в основе данного требования;
- каких проблем можно избежать, выполнив это требование;
- почему выполнение данного требования **принесет положительный эффект;**
- кто будет отвечать за выполнение данного требования.

Приложение 1
Этапы оснащения объекта системами безопасности

Работы по оснащению объекта системами безопасности проводятся поэтапно и в соответствии с утвержденными руководством заказчика концепцией, техническим заданием и выполненной, на его основании, проектно-сметной документацией.

1 этап. Предпроектная работа

1. Обследование и изучение особенностей деятельности объекта с точки зрения его безопасности (особенности функционирования, его местонахождение, уровень криминогенной обстановки, рельеф местности, климатические условия, окружающая обстановка, наличие системы безопасности, характеристика системы электроснабжения, помеховая обстановка и т.п.).

2. Аналитическая работа:
- оценка угроз;
- распределение по степени важности отдельных зон и направлений;
- выбор схемы взаимодействия технических средств защиты и личного состава охраны.

3. Разработка технико-экономического обоснования (технико-экономических предложений, технического задания на проектирование и т.п.):
- разработка структурной схемы комплекса;
- выбор номенклатуры, количества аппаратуры, вспомогательного оборудования;
- выбор типов кабелей, способов их прокладки;
- укрупненные сметные расчеты затрат (проектирование, согласование, приобретение аппаратуры, монтаж, наладка).

2 этап. Рабочее проектирование

Разработка комплекта рабочей проектно-сметной документации.

3 этап. Оснащение объекта

1. Приобретение аппаратуры, кабельной продукции, коммутационных изделий, монтажных материалов (при необходимости - изготовление нестандартного оборудования) и т.п.
2. Комплектование и поставка на объект.
3. Строительная подготовка объекта (устройство закладных элементов, деталей, строительно-планировочные работы и т.п.).
4. Установка и монтаж аппаратуры, оборудования, соединительных кабелей, кроссового оборудования, заземления и т.п.
5. Наладка аппаратуры, комплексная проверка и запуск.
6. Рабочий прогон смонтированного оборудования и предъявление к сдаче.
7. Выпуск исполнительской документации.
8. Сдача-приемка в эксплуатацию.

4 этап. Подготовка персонала

1. Подготовка внутриобъектовой нормативной документации.
2. Подбор кадров, формирование служб.
3. Обучение обслуживающего персонала правилам эксплуатации систем комплекса.
4. Разработка вводных задач, практических мер и сценариев действий личного состава службы безопасности и сотрудников охраны к действиям при штатных и нештатных ситуациях.

5 этап. Эксплуатация комплекса

1. Техническая и оперативная эксплуатация комплекса.
2. Проведение плановых регламентных работ, технического обслуживания в соответствии с требованиями эксплуатационной документации на аппаратуру.
3. Проведение плановой оперативно-технической учебы и практических занятий с личным составом по разработанным сценариям действий.

Примечания.

1. В приведенном алгоритме не учтены специфические этапы сметно-договорных работ (заключение договоров, порядок финансирования и т.п.).
2. Для сокращения сроков выполнения работ отдельные этапы могут быть совмещены (например, рабочее проектирование и приобретение устанавливаемого комплекта оборудования, оснащение и подготовка к эксплуатации и т.п.).
3. Подбор кадров и формирование служб (на 4 этапе) может проводиться заранее.

<u>Приложение 2</u>

Категории объектов, их состав и системы, рекомендуемые

	СОС - Система охранной сигнализации
	СТН - Система телевизионного наблюдения
	СОО - Система охранного освещения
Периметральное ограждение объекта:	С С - Система связи
- ограждение	СЭП - Система энергопитания
- ворота	СИТЗ - Система инженерной защиты
- КПП	СКНС - Система контроля несения службы
	СКП - Система контроля прохода на территорию
	СФНА - Система фиксации номеров автомашин
	СРП - Система резервного питания
Территория объекта:	СТН - Система телевизионного наблюдения
- склады	СОО - Система охранного освещения
- площадки хранения материальных ценностей	СОС - Система охранной сигнализации
- автостоянки	СКНС - Система контроля несения службы
- административные здания	СРП - Система резервного питания

	СОС - Система охранной сигнализации СПС и СОП - Система пожарной сигнализации и оповещения о пожаре
Объекты:	СТН - Система телевизионного наблюдения
- производственные здания	САПТ- Система пожаротушения
- административно-хозяйственные здания	СРП - Система резервного питания
	СКУД - Система контроля и управления доступом
- гаражи	САО - Система аварийного освещения
	СИТЗ - Система инженерной защиты

Анализ уязвимости объекта и оценка угроз

Уязвимость (объекта) - степень несоответствия принятых мер защиты (объекта) прогнозируемым угрозам или заданным требованиям безопасности.
Общая стратегия предотвращения краж и поджогов в магазинах и офисах должна рассматривать ситуации, когда помещения открыты для работы и когда они закрыты.
Основными направлениями в стратегии должны стать следующие:

• ограничение, насколько это возможно, числа наружных дверей, доступных окон и других путей возможного проникновения на объект;
• обеспечение, если это возможно таких условий, при которых потенциальный поджигатель не мог бы проникнуть на объект незамеченным;
• обеспечение освещения, достаточного для наблюдения за действиями нарушителя;
• установка и поддержание в рабочем состоянии запирающих устройств на наружных дверях, окнах и других возможных путях проникновения;
• контроль за доступом посетителей в помещения, не предназначенные для посещения клиентов в течение рабочего дня;
• планирование внутреннего расположения помещений таким образом, чтобы минимизировать потери от краж;
• увеличение, при необходимости, численности охраны;
• принятие мер к ограничению возможности возникновения пожара с внешней стороны объекта.

Чаще всего простой ответ на управленческие аспекты безопасности отсутствует, хотя желательно утвердить основные принципы, которым должны следовать менеджеры, охрана, сотрудники объекта.
При предварительной проработке вопросов основное внимание следует уделить:
• степени зависимости безопасности от архитектурно-планировочных решений объекта;
• влиянию места расположения на меры безопасности, учитывающему изолированность зданий (если это сельская местность), виды преступлений, совершаемые в данном районе (если здание находится в городе) или другие особенности (если здание находится в пригороде);
• существующему или потенциальному уровню и характеру преступности в данном месте (например, кражи со взломом, просто кражи, ДТП, вандализм и т.д.);
• близости к местам большого скопления народа (стадионы, дискотеки, пансионаты, гостиницы и др.);
• степени зависимости безопасности от природных и погодных условий, времени года, или сезонных факторов, например, потоков туристов;
• возможности использования природных факторов защиты, например, рек, водохранилищ, гор и др.;

• преимуществам, которые имеют место, где постоянно присутствуют люди (милиция, скорая помощь, пожарные), либо искусственные препятствия в виде решеток, оград и т.п. сооружений;
• организации уличного освещения;
• фактору видимости, т.е. расстоянию, с которого видно соседний объект.

Кроме вышеперечисленных факторов, необходимо учитывать возможное несанкционированное проникновение использующих средства обслуживания, например, грузовые лифты, места хранения подсобных материалов, вентиляционные люки, мусоропроводы и др. При приеме посетителей необходимо создавать специальные зоны, где они могут получить необходимую информацию Операционные стойки должны обеспечивать персоналу обзор этих зон.

Рассмотрение функций и конструкций дверей, окон, запоров - это совершенно самостоятельный раздел, напрямую связанный с технической безопасностью объектов, строительными и эстетическими требованиями, которые очень часто бывают взаимно исключающими.

Потолочные и коммуникационные пустоты также могут быть использованы в преступных целях, поэтому эти площади необходимо обеспечить защитой в той или иной форме. Это может быть физическая защита, препятствующая проходу, или система сигнализации, обнаруживающая проникновение.

Цели и задачи анализа

Проведение специалистами систематического анализа уязвимости объекта и существующей системы обеспечения его безопасности является одной из главных задач службы безопасности.
Целями и задачами проведения такого анализа являются:
• определение приоритетных объектов защиты, т.е. наиболее вероятных целей посягательства преступников;
• рассмотрение вариантов возможных угроз и моделей их реализации;
• оценка возможного ущерба;
• оценка уязвимости объекта и уровня надежности системы безопасности;
• разработка мероприятий по усилению безопасности объекта;
• учет изменений, произошедших в планировке и хозяйственной деятельности. Результаты анализа по указанным направлениям оформляются документально.

Количество экземпляров и гриф конфиденциальности определяется исполнителем. К ознакомлению с материалами анализа допускается только ограниченный круг лиц (по существующей на предприятии разрешительной системе).

Оценка угроз

Для различных предприятий, в зависимости от особенностей профиля деятельности, существует различный набор ресурсов и соответствующие им прогнозируемые угрозы безопасности. Важными для жизнедеятельности ресурсами, а, следовательно, объектами защиты являются:
• люди (персонал предприятия);
• имущество;
• важное или дефицитное технологическое оборудование;
• секретная или конфиденциальная документация;<
• материальные и финансовые ценности;
• готовая продукция;
• интеллектуальная собственность (ноу-хау);
• средства вычислительной техники <СВТ);
• конфиденциальная информация на материальных носителях, а также циркулирующая во внутренних коммуникационных каналах связи и информации, в кабинетах руководства предприятия, на совещаниях и заседаниях;<
• финансово-экономические ресурсы, обеспечивающие эффективное и устойчивое развитие предприятия (капитал, коммерческие интересы, бизнес-планы, кадровая статистика, договорные документы и обязательства и т.п.).

Основными угрозами, которые могут привести к значительному урону, являются:
- чрезвычайная ситуация (пожар, разрушение, затопление, авария);
- хищение опасных веществ и т.п.;
- хищение или порча имущества;

- несанкционированный съем конфиденциальной информации из защищаемых помещений;
- утечка информации по техническим каналам;
- ухудшение эффективности функционирования средств ТСО.
Реализация перечисленных угроз может привести:
- к созданию угрозы для жизни и здоровья людей;
- к катастрофическим последствиям для окружающей среды и населения;
- к большому материальному ущербу;
- к разглашению конфиденциальной информации или сведений, содержащих коммерческую тайну;
<- к банкротству предприятия.

В современных условиях несанкционированные действия физических лиц могут привести к возникновению большинства прогнозируемых угроз.
На этапе анализа угроз совместно со службой безопасности предприятия при предварительном обследовании объекта формируется модель вероятных исполнителей угроз (нарушителей), т.е. их количественные и качественные характеристики (оснащенность, тактика действий и т.п.) с учетом местных особенностей каждого предприятия.

Оценка возможных угроз производится по следующим направлениям (в приоритетной последовательности):
- безопасность персонала и посетителей;
- сохранность материальных ценностей, имущества и оборудования;
- безопасность информации, сохранность тайны.
Такая последовательность соответствует современным мировым нормам безопасности.

Определение приоритетов в расстановке акцентов в перечисленных направлениях зависит от специфики объекта, наличия и соотношения предметов защиты, а также конкретных оперативных задач, поставленных службой безопасности. Объективность в оценке угроз достигается за счет:
- анализа статистических данных о происшествиях и подсчета ущерба по каждому виду угроз;
- оценки оперативной обстановки на объекте и вокруг него;
- анализа угроз по аналогичным объектам.

Приоритеты видов угроз распределяются следующим образом:
- пожары, аварии и терроризм, стихийные бедствия;
- кражи материальных ценностей;
- кражи интеллектуальных ценностей;
- халатность.

Несмотря на существенное различие в характере угроз, создание защиты от каждой из них должно идти в комплексе с общей концепцией безопасности.
Первым шагом на пути обеспечения безопасности является осознание объема риска и его оценки. Для получения такой оценки надо представить различные варианты действий злоумышленника. Исходя из этих оценок, и принимаются соответствующие меры по обеспечению безопасности.

На профессиональном языке слово «риск» означает возможность нежелательного отклонения от требуемой (нормальной) ситуации, которое может быть вызвано злоумышленником. Для оценки полного объема риска и подготовки рекомендаций по обеспечению безопасности объект должен быть тщательно обследован. Необходимо помнить, что чем выше стоимость имущества или информационных средств, которые могут подвергнуться нападению, тем выше стоимость предпринимаемых мер защиты.

Меры по обеспечению безопасности неизбежно связаны с экономическими и практическими ограничениями, которые не поддаются точному определению. Поэтому предел ответственности в значительной степени зависит от юридической концепции того, что является обоснованным в тех или иных обстоятельствах. Основной задачей в охране объектов является сдерживание, а оружием - время. Необходимо обратить внимание на два аспекта оперативной деятельности: активный, принадлежащий человеку, и пассивный, относящийся к техническим средствам. Время, выигранное технической системой обнаружения нарушителя, должно обеспечивать наряду охраны возможность своевременного прибытия на место происшествия.

Обеспечение безопасности объектов является комплексной проблемой, связанной с решением ряда частных, но взаимосвязанных задач. Наиболее очевидные из них - вопросы инженерной укрепленности, подбора и расстановки технических средств (охранной и пожарной сигнализации, теленаблюдения и

др.), организации службы охраны, разработки требований по 8нутриобъекто80му и пропускному режиму, а также передачи и отображения информации.

При проектировании системы безопасности необходимо принимать во внимание психологию преступника: будет ли достигнут им положительный результат при попытке совершения кражи и какие возможные последствия ожидают его в случае отрицательного результата. Главная цель (одна из задач) созданной системы безопасности - наглядно представить ее возможности так, чтобы убедить преступника в том, что у него ничего не выйдет.

Создание комплекса инженерно-технических средств охраны (ТСО) одного или группы объектов ставит задачи не только их защиты, но и обмена информацией о состоянии технических средств и об оперативной обстановке. Функции обеспечения контроля пространственно рассредоточенных объектов возможны только при наличии разветвленной информационной сети, использующей различные виды и каналы связи.

Общие рекомендации по обеспечению безопасности объекта

В зависимости от количества объектов, подлежащих охране, их назначения и территориального расположения, характера и количества хранящихся в них материальных и информационных ценностей, возможностей физического реагирования на экстремальные ситуации, комплекс безопасности объекта будет включать в себя те или иные подсистемы. При решении вопросов оснащения объектов техническими средствами используются критерии, изложенные в государственных и нормативных документах МВД РФ.

Один из традиционных путей решения проблемы - увеличение персонала службы безопасности. Однако неоправданное увеличение количества людей создает свои проблемы.
С *одной стороны, люди - это наиболее дорогостоящая и нестабильная составляющая часть системы безопасности* (для обеспечения требуемой надежности их самих необходимо контролировать). *С другой стороны, люди являются обязательной составляющей частью любой системы безопасности.* Основной задачей при этом является создание оптимальной («по количеству и качеству») службы физической охраны, умеющей грамотно использовать технические средства и действовать в различных ситуациях. Для нормально-достаточной охраны больших объектов нужно круглосуточно иметь, как правило, от 5 до 15 штатных сотрудников охраны. Вопросы разработки инструкций для личного состава, механизмов их реализации и контроля требуют больших усилий и самого пристального внимания.

При установке на объекте большого количества технических средств охраны (ТСО) происходит значительное увеличение потока информации, что обычно создает высокую вероятность совершения персоналом ошибочных действий. В то же время задачей комплексной системы безопасности является максимальное упрощение управления системой с максимально наглядной информацией от подсистем и передачей технике всей рутинной работы, оставляя за людьми только функции принятия решений.

Основные факторы, определяющие эффективность работы комплекса технических средств:
• выдача "Тревожных» и предупреждающих сообщений и/или сигналов при выявлении нештатных (несанкционированных, неадекватных и др.) действий;
• объективное фиксирование текущей и оперативной информации от систем;
• выполнение охранных функций и выдача сообщений на центральный пульт охраны;
• работа в автономном режиме от дополнительных и/или центрального пульта охраны;
• выработка команд и сообщений по управлению всеми системами комплекса технических средств;
• объективный контроль действий персонала с возможностью их последующего анализа;

• сбор, архивирование, обработка информационных сообщений от систем, входящих в КСБ;
• стабильное функционирование технических средств КСБ.

Выбор технических средств защиты организациями, не имеющими в своем штате технических специалистов, носит случайный характер и может привести к существенному урону безопасности объекта, т.к. в этом случае потребитель ориентируется только на рекламные проспекты, что приводит к неоправданной трате денежных средств и, как следствие, к неэффективному использованию аппаратуры.

При решении вопроса, какие технические средства, отечественные или импортные, выбрать для систем безопасности, следует обратить внимание на полноту реализуемых ими функций. Часто зарубежные системы представляют собой либо систему контроля доступа с урезанной функцией охранной сигнализации, либо систему охранной сигнализации с урезанной функцией контроля доступа. Для облегчения выбора используемых систем необходимо сравнить их тактико-технические данные, основные из которых приведены в **Приложении 3.** Другие системы, входящие в комплекс защиты, устанавливаются, как правило, независимо и интегрируются в общий комплекс на уровне управляющих сигналов. Условием для интегрирования в комплекс какого-либо дополнительного оборудования является наличие у него коммуникационного порта (RS-232, RS-485) с соответствующим протоколом обмена. Основными узлами, на уровне которых осуществляется интегрирование, входящих в комплекс систем, являются программируемые контроллеры и/или приемно-контрольные приборы (панели), управление и передача данных от которых осуществляется по локальным информационным шинам. Необходимо отметить, что доработка импортного программного обеспечения для аппаратно-программной интеграции систем различных производителей, как правило, связана со значительными временными и финансовыми затратами и приводит к изменению условий штатной эксплуатации, определенных заводом-изготовителем.

Программное обеспечение комплекса должно располагать полным протоколом команд каждой из подсистем, а это неочевидная задача, т.к. маркетинговая политика многих производителей аппаратуры охранно-пожарной сигнализации не предусматривает распространение в том или ином виде системных кодов. Вопрос отладки такого программного продукта - длителен и трудоемок.

Подобно любым инвестициям, комплексная система безопасности должна окупаться: затраты на защиту от угрозы не должны превышать предполагаемый ущерб. Задача эта не простая. Так, пожарная система сигнализации может всю жизнь простоять на объекте и ни разу не сработать, но если она хотя бы один раз во время выдаст сигнал тревоги, то все затраты на нее сразу окупятся. С одной стороны, можно пойти по пути максимального насыщения объекта различными системами охраны с широким спектром функциональных возможностей, с другой - можно использовать минимальное количество аппаратуры, выполняющей общие задачи защиты объекта. Необходимо отметить, что снижение затрат на оборудование всегда означает отказ от некоторых защитных функций. Необоснованная экономия на первичных затратах приводит к увеличению эксплуатационных расходов и к снижению эффективности системы.

Выбор систем защиты и состава аппаратуры для комплекса по каждому конкретному объекту должен отвечать принципу необходимости и достаточности.

<u>Приложение 3</u>

Основные параметры сравнения систем

Для объективного сравнения систем, предполагаемых для использования в комплексе технической безопасности, при проведении тендера, целесообразно использовать критерии, обусловленные тактико-техническими данными предлагаемой аппаратуры.
Исходные данные для расчета необходимого состава аппаратуры по объекту:
• защищаемая площадь, м^{г};
• количество этажей в здании;
• общее количество помещений;
• наличие чердаков, подвалов;
• количество входов (выходов);
• количество помещений складов;
• количество особо важных помещений, вход в которые ограничен;
• общее количество сотрудников;

• общее количество людей, одновременно находящихся в здании;
• объекты контроля системы теленаблюдения;
• необходимость децентрализованной «постановки/снятия» с охраны помещений с помощью индивидуальных считывателей или групповых пультов;
• наличие на объекте электроснабжения по 1 группе надежности;
• возможность перспективного развития объекта в %;
• необходимость теленаблюдения по периметру и площади;
• уровень освещенности охраняемой территории;
• цифровая запись видеоизображений от ТВ-камер по сигналам "Тревога»;
• время архивирования видеоизображений;
• скорость записи видеоизображений - не менее 6 кадров/с;
• одновременная запись «тревог» от ТВ-камер.

Для защиты объекта в состав комплекса должны входить следующие системы технической безопасности:
• охранно-тревожной сигнализации;
• пожарной сигнализации и оповещения о пожаре;
• пожаротушения;
• телевизионного наблюдения;
• аварийного освещения;
• оперативной связи (проводной и радио);
• контроля прохода (входа/выхода) в здание;
• контроля доступа в выделенные помещения объекта.

Параметры сравнения систем

При выборе технических систем защиты необходимо предварительно убедиться в наличии на каждую систему следующей документации, после чего сравнить их по приведенным ниже параметрам:
• сертификатов соответствия: ГОСТ Р и пожарной безопасности на систему и все блоки, входящие в ее состав;
• сертификата ISO 9001 (для импортных систем);
• полного комплекта эксплуатационно-технической и ремонтной документации на русском языке;
• русифицированного программного обеспечения и отображения информации на блоках контроля и управления;
• лицензий на проектирование и монтаж соответствующих систем;
• наличие предлагаемого оборудования в перечне МВД РФ;
• расчета эффективности использования базового комплекта аппаратуры для защиты заданного количества объектов.

Система охранной сигнализации:

• фирма, страна производитель;
• наличие промышленного серийного производства;
• минимальная и максимальная емкости системы;
• возможность расширения емкости;
• количество регистрируемых параметров;
• возможность стыковки с другими системами ИСБ;
• общее количество контролируемых системой шлейфов сигнализации;
• наличие выносных пультов программирования, контроля и управления;
• возможность организации нескольких АРМ;
• максимальная длина линии интерфейса RS - 485;
• количество команд, реализуемое по интерфейсу RS - 485;
• количество сообщений, передаваемых по интерфейсу на центральный пульт;
• среднее время наработки на отказ в "Дежурном» режиме;
• вероятность ложных срабатываний за 1000 часов работы в «дежурном» режиме;
• наличие в комплекте считывателей с режимом «постановки/снятия» и контроля доступа;
• устойчивость к воздействию электромагнитных помех;
• обеспечение пожарной безопасности в аварийном режиме;
• диапазон рабочих температур;
• наличие в техдокументации схем: структурной, принципиальной, входного контроля;
• состав и стоимость комплекта оборудования и ПО для защиты конкретного объекта;
• стоимость программного обеспечения.

Система пожарной сигнализации и оповещение о пожаре:

• фирма, страна производитель;
• тип системы (аналоговая, адресная, адресно-аналоговая);
• количество радиальных / кольцевых шлейфов;
• общее количество датчиков/блоков, подключаемых в шлейф;
• объем сохраняемой информации;
• наличие режима повышенной чувствительности (день/ночь);
• возможность управления системами пожаротушения и оповещения о пожаре;
• возможность организации нескольких АРМ;
• наличие адресных модулей: контроля, управления, шлейфов с традиционными датчиками;
• наличие блоков локализации КЗ;
• наличие выхода на персональный компьютер; ит.п.);
• наличие порта RS-232, RS-485, передачи информации на другие системы;
• количество независимо программируемых групп;
• возможность увеличения емкости системы от……до…..;
• возможность интегрирования с системой охранно-тревожной сигнализации, телевизионного наблюдения и контроля доступа;
• максимальная длина (сопротивление) шлейфа сигнализации;
• максимальная длина интерфейса RS-485;
• наличие выносных пультов управления;
• состав и стоимость комплекта оборудования и ПО для конкретного объекта;
• программное обеспечение для приема и отображения информации;
• программное обеспечение для передачи конфигурации системы на ПК;
• возможность управления и контроля инженерными системами здания.

Оповещение о пожаре:

• мощность усилителя низкой частоты (УНЧ);
• мощность используемых громкоговорителей;
• наличие тюнера;
• наличие магнитофонной деки;
• наличие режима оповещения (микрофон) и трансляции;
• наличие блоков управления, автоматики и сигнализации;
• диапазон воспроизводимых частот;
• величины напряжений на выходах УНЧ;
• наличие встроенных тональных генераторов;
• возможность установки в стандартный 19" шкаф;
• наличие таймера программного обеспечения;
• стоимость комплекта (с громкоговорителями);
• виды используемых громкоговорителей (потолочные, настенные, колонки и т.п.
• фирма, страна-производитель.

Система автоматического пожаротушения:

• фирма, страна производитель;
• состав и стоимость комплекта оборудования для защиты объекта общей площадью м. кв.;
• вид огнетушащего состава.

Система телевизионного наблюдения:

• тип используемых камер черно-белого/цветного изображения: аналоговые; цифровые;
• формат матрицы;
• разрешающая способность;
• чувствительность (по освещенности объекта);
• соотношение сигнал/шум;
• наличие автодиафрагмы;
• максимальное количество камер подключаемое к системе (компьютеру);
• минимальная суммарная скорость записи;
• алгоритм сжатия;

• объем памяти (в базовом варианте);
• формат мультиэкрана;

• наличие «стоп-кадра»;<
• возможность записи видеоизображения «до» и «после».....сек. до события;
• наличие встроенного генератора данных (дата, время, номер камеры);
• наличие встроенного детектора движения;
• наличие «тревожных» входов управляемых от других систем;
• наличие и количество выносных пультов управления;
• состав и стоимость комплекта системы для оборудования объекта.

Система оперативной связи:

Радиосвязь:
• фирма, страна производитель;
• возможность связи в N-этажном здании с ж/б перекрытиями;
• состав аппаратуры;
• максимальное количество радиопередатчиков;
• максимальная мощность радиопередатчиков;
• диапазон частот;
• количество каналов;
• время непрерывной работы;
• чувствительность радиоприемной станции;
• уровень побочных излучений;
• наличие кодирования;<
• стоимость комплекта;
• режим работы: дуплекс, полудуплекс.

2. *Проводная связь:*
• фирма, страна производитель;
• состав аппаратуры;
• максимальное количество абонентских точек;
• необходимость набора номера точки (абонента);
• стоимость комплекта оборудования.

Система аварийного освещения

(освещение безопасности или эвакуационное - при численности персонала более 50 человек):
• фирма, страна производитель;
• соответствие светильников НПБ 249-97 «Светильники. Требования пожарной безопасности. Методы испытаний»;
• типы используемых ламп;
• наличие источника автономного питания для эвакуационных светильников;
• наличие схемы переключения с нормального режима на резервный;
• максимальная потребляемая мощность эвакуационных светильников;
• возможность включения по сигналу «тревога» от системы охранно-пожарной сигнализации;
• количество и стоимость комплекта светильников (арматуры, пускорегулирующей аппаратуры и ламп) для объекта.

Система контроля доступа:

• фирма, страна производитель;
• контроль режима «вход-выход» по карточкам-пропускам;
• учет количества сотрудников (посетителей) прошедших через проходную;
• наличие режима учета рабочего времени;
• возможность создания единой сети считывателей;
• общее количество распределенных по объекту точек, контролируемых системой:
• возможность использования индивидуальных считывателей для «входа-выхода» в помещение и для его «сдачи-снятия» с охраны;
• максимальный объем информации, обрабатываемый системой за сутки (кол-во человек);
• количество проходов и регистрации за час;

• возможность использования турникетов в качестве шлюзов;
• наличие индикации (зел./красн.) разрешающей/запрещающей проход;
• программное обеспечение: системное и количество модулей для решения конкретных задач;
• возможность изменения алгоритма пропуска заказчиком;
• ресурс работы механической части системы;
• состав и стоимость оборудования и ПО.

Система бесперебойного электроснабжения:

• вид системы;
• мощность нагрузки;
• напряжение нагрузки;
• оптимальный ток нагрузки;
• время непрерывной работы при использовании: аккумуляторов; бензо/дизель агрегатов;
• наличие автоматического включения / пуска (при пропадании основного питания);
• время выхода на рабочий режим бензо/дизель агрегатов;
• фирма, страна производитель;
• стоимость.

Единый центр мониторинга и управления системой безопасности:

• габаритные размеры пульта;
• модульность конструкции;
• удобство эксплуатационного обслуживания;
• максимальное количество мониторов устанавливаемое в пульт;
• размеры экранов мониторов;
• соответствие оборудования и рабочих мест санитарным нормам;
• соответствие пульта требованиям технической эстетики по ГОСТ 24750-81;
• соответствие пульта общим эргономическим требованиям по ГОСТ 12.2.033-78;
• количество (в %%) оборудования КБО устанавливаемого в пульт;
• необходимость установки дополнительных шкафов и возможность их стыковки с пультом;
• возможность регулировки полок (рабочих мест аппаратуры) для установки конкретного оборудования;
• стоимость, страна - производитель.

Комплекс безопасности объекта

Подкомплексом безопасности объекта (КБО) понимается совокупность технических средств и систем (подсистем), работающих в единой программно - аппаратной среде (оборудование одного или нескольких производителей, реализующих полную техническую совместимость между собой отдельных приборов, блоков и программных модулей), обеспечивающей необходимый и достаточный уровень технической защиты объекта и своевременное получение информации о ее работе на различных уровнях.

Обоснование затрат на КБО может стать средством выявления неэффективных систем и принятия мер к их наиболее рациональному использованию. Выбор состава систем (подсистем), входящих в КБО, связан с оценкой их тактико-технических возможностей, цены и качества, которую могут дать специалисты соответствующей квалификации. Основные сравнительные характеристики систем, которые могут быть использованы при подготовке предложений по выбору аппаратуры для защиты объектов, приведены в Приложении 3.

В организациях с развитой сетью филиалов, связанных между собой компьютерными сетями, возможно создание объединенной системы безопасности, обеспечивающей ее поэтапное создание. Свойства модульности, наращиваемости и возможности удаленного подключения, обеспечивают возможность создания комплексной системы безопасности для любых объектов и расстояний. Эффективность КБО обеспечивается способностью распределенного принятия решений, т.е. стандартные задачи решаются на соответствующих уровнях систем, не загружая при этом центральный процессор. Правильная оценка информационно-пропускной возможности системы позволяет избежать неприятностей при инсталляции и эксплуатации КБО.

При выборе систем, образующих КБО, учитываются реальные и потенциальные угрозы, а также принцип "равной защищенности", предусматривающий построение такой системы, при которой каждая, входящая в нее подсистема имеет одинаковую эффективность. Современный подход к обеспечению надежности систем заключается в оптимизации соотношения между затратами на систему и эффективностью самой системы. При этом под эффективностью понимается среднее значение функции качества, описывающей работу системы во времени с учетом отказа ее отдельных элементов, которые сопровождаются тем или иным изменением качества. Методы обеспечения надежности в этом направлении можно условно разбить на основные группы:
- уменьшение интенсивности отказа элементов;
- уменьшение времени восстановления;
- сокращение периодов непрерывной работы до оптимального значения.

В случае программно - аппаратного объединения различных подсистем, КБО будет представлять собой единое целое, т.к. при выходе из строя, отключении оборудования или сбое программного обеспечения любой из систем остальные будут продолжать функционировать в нормальном режиме. В такой системе требование об обмене информацией в реальном масштабе времени необязательно. В данном случае комплексность подразумевает мониторинг и управление перечисленными подсистемами.

Для того, чтобы создание КБО было оправдано с финансовой точки зрения, целесообразно рассматривать все системы, входящие в комплекс, как единое целое. В этом случае, на этапе проектирования, можно уменьшить расходы и избежать дублирования функций за счет *единой структурированной кабельной сети* (СКС) и избыточности по оборудованию. КБО следует проектировать открытой системой, т.е. такой, которая позволяет стыковать ее с другими инфраструктурами объекта.

При проектировании КБО, как правило, выполняются следующие этапы:
• определение возможных форм управления;
• определение необходимых реакций на угрозы;
• определение структуры и составляющих подсистем;
• определение алгоритмов взаимодействия подсистем;
• интегрирование дополнительного оборудования;
• определение уровней и объемов передачи информации;
• составление и утверждение заказчиком технического задания;
• выбор оборудования с оптимальными характеристиками.

Общая структурная схема КБО

Структурная схема КБО в общем виде представляет собой пространственно распределенную радиально-кольцевую структуру, объединенную локальной системой связи.
Для создания системы безопасности рассредоточенных объектов и включения их в КБО необходимо, как минимум, чтобы каждый из них был оборудован хотя бы одной из систем: СОС, СПС, СТН, СКП. В зависимости от назначения объектов и находящихся в них материальных ценностей, состав систем и условия оборудования соответственно корректируются.

Наличие объектов с большими материальными или информационными ценностями требует дополнительного оборудования их системами фиксации въезжающего/выезжающего транспорта, контроля несения службы, ограничения доступа посторонних лиц. Необходимость установки той или иной системы определяется на этапе разработки технического задания, согласовывается со службой безопасности, учитывается при проектировании и реализуется при монтаже.

Условно, по значимости КБО может быть разделен на четыре уровня:
1 уровень (информационный) выполняет функции компьютерного контроля за системой, контроля за

работоспособностью пультов дистанционного управления и контроля, приемно-контрольных приборов, шлейфов сигнализации, исполнительных устройств.
Первый (высший) уровень КБО представляет собой компьютерную сеть типа клиент/сервер на основе сети ETHERNET с протоколом обмена tcp/ip и с использованием сетевых операционных систем Windows NT или Unix. Этот уровень обеспечивает связь между сервером и рабочими станциями операторов.
2 уровень (управляющий) выполняет функции дистанционного управления системой и контроля за работоспособностью приемно-контрольных приборов, шлейфов сигнализации, кабельных сетей, датчиков и исполнительных устройств.
Второй (управляющий и регистрирующий) уровень представляет собой пульты дистанционного управления и контроля, размещаемые на объекте и соединенные с центральным компьютером сетью с передачей по ней информации на 1 уровень по каналам RS - 232 (удаленный вариант), RS - 485. Второй уровень обеспечивает связь между контроллерами и компьютерами подсистем;
3 уровень (фиксирующий) комплект приемно-контрольных приборов и аппаратуры для управления и контроля за работоспособностью шлейфов сигнализации, кабельных сетей, датчиков и исполнительных устройств.
Третий (фиксирующий) уровень представляет собой комплект из приемно-контрольных приборов и аппаратуры различного назначения, обеспечивающей их работоспособность и соединенных пультами дистанционного контроля по кабельным сетям с передачей информации на 2уровень по каналам RS - 232 или RS - 485. Третий уровень обеспечивает связь между контроллерами и считывателями. Здесь, как правило, применяется интерфейс RS 485 или интерфейсы считывателей Wigand.
4 уровень (технологический) комплект шлейфов сигнализации, кабельных сетей, датчиков, исполнительных устройств.
Представляет собой комплект из датчиков с разными физическими принципами действия, шлейфов сигнализации, кабельных сетей, исполнительных устройств, соединенный с приемно-контрольными приборами, источниками питания, сигнальными и силовыми кабельными сетями и передающим по сетям информацию на 3 уровень в виде сигналов типа "сухой контакт". Четвертый уровень извещателей системы охранно-пожарной сигнализации и цепей управления. Как правило, здесь применяются нестандартные специализированные интерфейсы и протоколы (например, обмен информацией по адресным двухпроводным шлейфам).

Вместе с тем интеграция систем имеет и некоторые отрицательные стороны.
Во-первых, при решении вопроса об интеграции систем следует исходить из того, что интегрированная система безопасности должна обеспечить более высокую надежность. Этого можно добиться только при работе каждой из подсистем в автономном режиме, т.е. чтобы выход из строя любой из них не приводил к выходу из строя или неисправности всего комплекса.
Во-вторых, учитывая, что управление комплексной системой безопасности осуществляется с использованием компьютеров, передавать управление всей системой, с входящими в нее подсистемами, компьютерам нецелесообразно, т.к. компьютер является наименее надежным звеном системы. Для обеспечения высокой надежности системы безопасности требуется использование только специализированных компьютеров, свободных от выполнения других задач, а также применение различных методов резервирования системных ресурсов, баз данных и режима гарантированного питания. Кроме того, подсистемы КБО должны иметь распределенный интеллект, чтобы при выходе из строя одной из них остальные обеспечивали выполнение своих основных функций.
В третьих, сеть высшего уровня должна быть локальной (физически отделенной от остальных информационных сетей объекта). Для передачи данных в сети надо, при необходимости, использовать криптографические методы защиты информации, а также имитостойкие протоколы обмена информацией.

Реальное повышение эффективности функционирования комплексных систем безопасности достигается за счет использования метода раннего обнаружения несанкционированного проникновения (НП). Очевидно, что обнаружение НП и формирование извещения о проникновении в системе охраны объекта осуществляется подсистемой охранной сигнализации, основу которой составляют извещатели различных видов, назначения и принципа действия. Вероятность НП в значительной мере зависит от воздействия нарушителя на инженерно-физическую защиту объекта. Общее время несанкционированного проникновения складывается из суммы времени затраченного на преодоление технической укрепленности строительных и/или специальных инженерных конструкций объектов и длительности совершения правонарушения. Время задержания нарушителя состоит из времени его регистрации техническими средствами, времени передачи сигнала "тревога", обработки поступившей на центральный пульт информации и прибытия наряда к месту происшествия. Из этого следует, что одним из путей уменьшения вероятности НП является сокращение времени бесконтрольного нахождения

преступника на объекте, которое в общем случае состоит из продолжительности опосредованного (через строительную конструкцию) контакта нарушителя с извещателями охранной сигнализации и аппаратурного времени обнаружения. Поэтому применение технических средств, непосредственный контакт с которыми начинается с самого начала преодоления укрепляющих конструкций объекта, позволяет существенно уменьшить время обнаружения нарушителя и увеличить вероятность его задержания. Таким образом, вероятность пресечения НП может быть гарантирована только при минимальном времени прибытия к месту происшествия оперативной группы. Комплексное применение извещателей с различными принципами обнаружения нарушителя для защиты первого рубежа охраны (заборов, наружных стен, окон, дверей, люков и т.п. конструкций) не только обеспечивает защиту первого рубежа, но и позволяет организовать многорубежную охрану объекта.

Защита любого объекта, имея в виду закрытое помещение, начинается с его периметра (дверей, окон, люков, стен перекрытий и других строительных конструкций, средств инженерной укрепленности), т.е. с создания первого рубежа защиты охранной сигнализации.

Каждый объект охраны имеет свою самостоятельную систему безопасности с входящими в нее подсистемами, содержащими необходимый для них набор технических средств. Приемно-контрольный прибор или контроллер соответствующего уровня системы безопасности подключается при этом к локальной сети самостоятельно или через персональный компьютер. Связь между системой безопасности периферийного объекта и компьютером центрального пульта осуществляется по локальной системе связи.

При наличии на объекте нескольких самостоятельных зданий (дома, склады и т.п.), создаются самостоятельные системы охраны каждого объекта с выводом сигналов на локальный (периферийный) пульт, находящийся на этой же территории (в одном из зданий или на КПП) и подключенный через локальную сеть на центральный пульт.

Объекты, территориально расположенные на значительном расстоянии от центрального пульта, подключаются к нему по специальным линиям связи (ведомственным или абонируемым), обеспечивающим передачу необходимого объема информации.

На центральный пульт от рассредоточенных систем, как правило, передается минимальный объем информации - *сигналы "тревога"* и суточный отчет по установленной форме. При необходимости передачи соответствующих видеоизображений в реальном масштабе времени или в сжатом виде необходимо учитывать технические возможности имеющейся аппаратуры передачи и регистрации изображений и линий связи.

При необходимости, дежурный центрального пульта или руководство службы безопасности, могут получить интересующую их информацию о состоянии удаленных объектов, для этого их персональные компьютеры должны быть подключены к той же локальной сети связи.

Одним из вопросов, при создании КСБ, является выбор системы отображения информации в наглядном для оператора виде (в виде таблиц или графических планов объекта). Использование для этих целей одного, даже с очень большим экраном, монитора для получения информации сразу от всех систем, входящих в КБО нецелесообразно. Проблемами выбора системы отображения являются:
- сложность в реализации системы (взаимосвязь потенциальных угроз с выработкой алгоритмов взаимодействия компонентов КСБ);
- значительное усложнение алгоритмов взаимодействия с увеличением количества систем;
- необходимость ввода в штат сменных высококвалифицированных системных администраторов;
- представление большего объема информации в удобной для восприятия форме.

Основные функции КБО:

Система КБО должна обеспечивать выполнение следующих основных функций:
- пассивного регулирования и предупреждения;
- обеспечения пожарной безопасности;
- наблюдения, обнаружения и оповещения;
- локализации и устранения угроз;
- управления эвакуационно-спасательными средствами;
- связи и аварийной системы передачи информации;

- аварийного разблокирования устройств ограничения доступа (шлагбаумов, турникетов):
- выдачу управляющих сигналов на инженерные системы жизнеобеспечения.

Таблица 1. Требования к уровню помехозащищенности

Аппаратура	Показатели помехозащищенности		
	Напряжение помехи, В	Длительность помехи, мс	Характер помехи
Приемно-контрольные приборы, контроллеры	160	200-250	Апериодический
Извещатели	160	не менее 250	Апериодический

Основные факторы, определяющие эффективность работы КБО:
- степень ориентации системы на выявление факторов риска (тревоги);
- правильный выбор и размещение компонентов системы;
- определение способа/ уровня интеграции (состав и назначение межсистемных связей);
- параметры регистрируемых сообщений, оптимизация вида и состава отчетов комплекса;
- уровень автоматизации реакций системы на нарушение;
- коммуникационные параметры аппаратно-программных средств КБО (адаптивность платформы к распределенной инфраструктуре объекта).

Особенности систем комплекса:
- независимое управление зонами охраны с использованием специальных контроллеров и считывателей;
- постановка и снятие с охраны объектов через элементы системы управления доступом;
- использование графических планов объекта для управления и отображения состояний системы;
- высокий уровень автоматизации функционирования, управления и регистрации;
- возможность включения в локальную информационную сеть;
- централизованный мониторинг.

При проектировании КБО необходимо также предусматривать варианты частичного функционирования системы (с ограниченными возможностями), алгоритмы ремонта и последующего восстановления нормальной работы. В частности в составе системы должен быть ЗИП для срочной замены наиболее важных узлов или компонентов, имеющих наибольшую вероятность выхода из строя, специально обученный персонал для планового обслуживания и ремонта системы; способы ремонта оборудования, возможность его замены необходимо проработать заранее

Большое внимание в эффективном использовании КБО должно уделяться оператору, который фактически является частью системы "мащина-человек" - с одной стороны он исполняет функции аппаратного фиксирования и оценки событий, с другой - функции посредника по принятию решений и их реализацией сотрудниками охраны. Нормальный, специально нетренированный человек-оператор может воспринимать поступающую информацию не более чем по 5-6 информационным направлениям, а оперативно реагировать только по одному. Выбор этого, одного направления, часто бывает не самым правильным, что в ситуациях с жестко ограниченными временными интервалами приводит к неадекватной реакции оператора на произошедшее событие и, как следствие, к трудно предсказуемым последствиям. Оператор КБО должен пройти подготовку:
- по работе с установленной техникой;
- по изучению ее тактико-технических параметров;
- по выполнению типовых алгоритмов реагирования;
- по отработке стандартных тревог от разных систем;
- по принятию решений в экстремальных ситуациях.

По каждому объекту, с учетом его особенностей, для оператора должны быть подготовлены и утверждены руководством службы охраны подробные инструкции реагирования на различные ситуации.

Периодическое проведение учебных тревог с использованием вариаций этих ситуаций способствует повышению профессионального уровня подготовки операторов.

Каждый оператор, работающий с системой, должен иметь свой персональный идентификатор, с использованием которого он может управлять системой только в рамках заданных для него полномочий. При этом все его действия в системе строго персонифицируются. Введение новых идентификаторов и присвоение полномочий могут осуществляться только специально уполномоченным лицом (начальником службы безопасности или охраны).

Системой КБО должна предусматриваться возможность автоматической проверки наличия оператора на рабочем месте. При этом система по псевдослучайному закону запрашивает оператора и просит подтвердить его присутствие на рабочем месте.
Необходимо помнить, что КБО - является только технической составляющей всей системы безопасности объекта.

Системы технической безопасности КБО

Комплекс безопасности объекта (КБО) включает в себя, как правило, следующие подсистемы:
- охранно-тревожная сигнализация (СОТС);
- пожарная сигнализация и оповещение о пожаре (СПС и СОП);
- автоматическая система пожаротушения (САПТ);
- охранное телевидение (СТН);
- охранное освещение (СОО);
- контроль прохода на объект (СКП);
- контроль доступа и управления доступом в помещения (СКУД);
- контроль несения службы (СКНС);
- оперативная связь (СОС);
- система фиксации номеров автотранспорта (СФНА);
- инженерно-техническая защита (СИТЗ).

В КБО могут входить и другие системы, которые будут дополнять и взаимодействовать с указанными. С учетом имеющихся потребностей, перспективных планов, и других факторов, определяется необходимый набор подсистем. При этом следует учитывать реальные и потенциальные угрозы объекту, а также принцип "равной защищенности". Этот принцип предусматривает построение такой комплексной системы, которая обладает примерно одинаковой эффективностью всех, входящих в нее подсистем. Объединение всех подсистем в единую систему является сложной организационной и инженерной задачей.

Рассматривая перечисленные выше системы технической защиты видно, что в основном они направлены на обнаружение угроз материальным ценностям и оборудованию. Необходимо отметить, что каждая из указанных подсистем может работать самостоятельно. Однако при оборудовании объектов техническими средствами защиты желательно интегрировать их в единую систему. Такая система усиливает свои защитные свойства за счет возможностей каждой из систем. Ядром комплексной системы являются средства интеграции и управления. Большое количество технических средств приводит к увеличению потока информации об обстановке на объекте, что влечет за собой высокую вероятность совершения персоналом ошибочных действий. Необходимо помнить, что средства интеграции должны:
- вести объективный контроль действий персонала;
- выдавать предупреждающие сигналы в случае выявления нештатных ситуаций;
- выдавать оперативную информацию по обстановке на объекте;

- выполнять охранные функции и выдавать сообщения на центральный пульт охраны;
- работать в автономном режиме при потере управления;
- выдавать команды и сообщения по управлению всем комплексом;
- регистрировать, обрабатывать и архивировать информацию от систем, входящих в комплекс;
- контролировать работоспособность технических средств, входящих в комплекс.

Так, при срабатывании пожарных дымовых извещателей, может сработать и охранный извещатель, установленный в том же помещении, подтверждая сигнал тревоги от пожарной сигнализации, при этом могут также автоматически включиться система дымоудаления, пожаротушения, инженерного и, лифтового оборудования, а система контроля доступа разблокирует замки эвакуационных дверей. С помощью телевизионных камер также можно наблюдать появление дыма в соответствующих помещениях. Из приведенного примера видно, что одним из главных достоинств такой системы безопасности является повышенный уровень достоверности информации и возможность оперативного принятия первоочередных мер по минимизации потерь и ущерба.

Интегрированные в единую структуру технические средства и программное обеспечение систем безопасности представляют собой комплексную систему сбора информации, обеспечивающую достаточную адресность, необходимую для оперативного вмешательства физической охраны.

Комплекс безопасности, кроме перечисленных функций, позволяет также осуществлять контроль и регистрацию состояния сигнализации охраняемых объектов, автоматическое обнаружение и фиксацию опасных ситуаций, управление инженерными системами, административный контроль и управление.

Этапы создания КБО

Прежде чем рассматривать системы, входящие в комплекс безопасности технических средств необходимо остановиться на требованиях нормативно-технической документации определяющих этапы работы по его созданию:
- обследование объекта защиты;
- разработка и согласование технического задания на проектирование и проведение технико - экономического обоснования <ТЭО);
- разработка и согласование проектной документации;
- монтажные и пусконаладочные работы;
- приемка работы.

При обследовании объекта на предмет оборудования его техническими средствами защиты целесообразно воспользоваться рекомендациями, изложенными в пособии "Порядок обследования объектов принимаемых под охрану. Методическое пособие" (издание НИЦ "ОХРАНА" МВД РФ). По результатам такого обследования оформляется акт, на основании которого, а также в соответствии с РД 25.952-90 составляется и утверждается техническое задание (ТЗ) на проектирование. После этого проводится технико-экономическое обоснование (ТЭО) выбранного варианта. Утвержденное ТЗ является основанием для начала проектных работ.
Проектная документация должна отвечать требованиям действующих нормативных документов.

Основные технические средства защиты объектов

Система охранно-тревожной сигнализации (СОТС)

Система СОТС обычно строится по схеме с распределенной архитектурой. Управление работой и отображение состояний системы (на 1 высшем уровне) осуществляется на компьютерном терминале с использованием графических планов объектов с разными уровнями детализации.
Распределенная архитектура обеспечивает создание адресной охранно-тревожной системы с сохранением широкого набора функциональных возможностей, присущих только специализированным системам. При этом увеличивается надежность и живучесть всей КСБ, оптимизируется кабельная сеть.
На каждом объекте к приемно-контрольной аппаратуре возможно подключение широкого спектра датчиков, использующих различные физические принципы обнаружения.
При наличии нескольких рассредоточенных объектов связь их периферийных пультов с центральным пультом осуществляется через специализированный контроллер с использованием протокола высокого уровня защищенности.
Классификация объектов по группам защиты, в зависимости от хранящихся на них материальных ценностей приведена в **Приложении 4.**

Основным назначением системы охранно-тревожной сигнализации является:
• выдача сигнала "тревога" при попытке несанкционированного проникновения в зоны, защищаемые техническими средствами охраны;
• подача тревоги при чрезвычайных ситуациях;
• ведение и архивация протокола событий, состояния системы и действий оператора с указанием времени и даты;
• выдача сигналов управления на исполнительные устройства (световые и звуковые оповещатели, охранное освещение, коммутация телевизионных камер и т.д.).

Необходимо помнить, что охранная сигнализация не задерживает нарушителя, она только информирует службу охраны о несанкционированном проникновении и месте его совершения.

Как правило, система охранной сигнализации состоит из двух основных компонентов: извещателей (датчиков) и приемно-контрольных приборов (контроллеров). Сигналы о срабатывании датчиков фиксируются, обрабатываются и передаются через промежуточные устройства или непосредственно на приемно-контрольный прибор (контроллер).

Основанием для принятия решений по уровню защиты средствами сигнализации тех или иных помещений являются требования нормативных документов МВД РФ. При этом, в первую очередь, необходимо принимать во внимание состав и количество материальных ценностей, находящихся на объекте, вид и значимость охраняемого объекта, принятую тактику охраны, электромагнитную обстановку на объекте в целом, технические характеристики используемого оборудования **(Приложение 5).**

При включении системы охранной сигнализации, использующей персональный компьютер, в комплекс системы безопасности, появляется ряд дополнительных преимуществ и возможностей:
• создавать и модифицировать графические планы объекта с различной степенью детализации и размещать на них условные обозначения различных элементов безопасности, выводить на экран графические планы объекта различного масштаба;
• постоянно контролировать состояние технических средств с протоколированием событий;
• отображать на экране монитора сведения о неисправности системы;
• просматривать состояние системы на общем и детализированном плане объекта;
• управлять системой сигнализации, используя графические планы объекта;
• автоматически выделять на плане объекта тревожные зоны, сопровождая это звуковым сигналом;
• верифицировать достоверность происхождения события через ТВ-систему, входящую в комплекс безопасности, обеспечивая приоритетность видеорегистрации этих изображений;
• автоматически выводить на экран операторов сообщения, рекомендации, инструкции по конкретному событию;
• вести протокол происходящих событий, просматривать и выводить на принтер информацию с фильтрацией по заданным критериям;
• контролировать несение службы персоналом охраны.
В то же время использование компьютеров в системах охраны требует соответствующего уровня подготовки дежурного оператора, как в профессиональном, так и в техническом плане.
Выбор способов защиты помещений определяется следующими факторами:
• соотношением стоимости защиты и возможных потерь;
• надежностью выбранной схемы защиты;
• стоимостью {денежной или иной) охраняемого имущества.

Система охранной сигнализации периметрального ограждения объекта

Проблема безопасности любого объекта должна решаться на основе концептуального подхода с целью создания целостной системы защиты, включающей в себя взаимосвязанные организационные, технические и оперативные меры.
В теории безопасности разработан комплекс базисных положений, являющихся основой при построении любой системы безопасности, применимых, в том числе, и для системы охраны периметра. Основные из них:
• комплексный подход, обеспечивающий оптимальное сочетание и взаимодействие всех средств, систем и процедур функционирования систем безопасности;
• система безопасности не должна причинять вред жизни и здоровью человека;
• применяемые средства и методы защиты должны быть достаточны и адекватны возможной угрозе;
• меры противодействия должны быть дифференцированными, т.е. распределенными в соответствии с вероятностью угроз и важностью защищаемой зоны;
• сигнал тревоги должен поступать как можно раньше, чтобы было время для адекватного реагирования на него;
• используемые технические средства и системы не должны создавать препятствий для нормального функционирования объекта.

Необходимо отметить, что универсальной системы защиты для всех объектов, расположенных в разных природно-климатических и географических условиях, не существует. Выбор той или иной системы зависит от множества факторов характерных для того или иного объекта, основные из которых сводятся к следующему:
• способы преодоления сигнализации периметрального ограждения, с учетом потенциальных возможностей;
• наличие инженерной защиты периметра {материал, высота, прямолинейность трассы, изменение высот внутри и снаружи);
• наличие и размеры "полосы отчуждения";
• характер грунта, возможности использования его для преодоления периметра;
• климатические особенности {температура, осадки, скорость ветра и т.д.);
• наличие и характер растительности в зоне периметрального ограждения;
• близость высоковольтных линий электропередач;
• пересечение периметра подземными и наземными магистралями (трубопроводами, эстакадами, канализационными каналами, коллекторами);
• количество и виды разрывов в ограждении (ворота, проезды, калитки). Комплекс периметральных инженерных сооружений для защиты объекта - это система ограждений, ворот и проходных. Охрана периметрального ограждения объекта - ключевой момент в предотвращении несанкционированного доступа на объект посторонних лиц.

Эффективность инженерных сооружений периметра определяется их надежностью и долговечностью. При разработке мероприятий по защите периметра необходимо:
• составить план - схему охраняемой территории (в масштабе) с указанием подъездных путей, соседних и примыкающих зданий и сооружений, выходов на поверхность подземных коммуникаций и т.д. для определения потребного количества технических средств;
• нанести на план - здания и сооружения, подъездные пути к ним;
• произвести деление объектов по степени важности для обеспечения их инженерной защиты {например, трансформаторные подстанции, склады материальных ценностей, ГСМ и т.п.);
• произвести контроль и оценить:
- ландшафт (по высотам, наличию растительности ит.д.);
- климатические условия {по количеству выпадающего снега, возможности подъема воды и т.д.);
• смонтировать инженерные сооружения {ограждения, ворота и т.п.);
• установить систему охранной сигнализации периметрального ограждения;
• учесть состояние криминогенной обстановки в данной местности.

Система пожарной сигнализации и оповещения о пожаре

Основным назначением пожарной сигнализации является:
• выдача сигнала "тревога" при возникновении признаков загорания (температура, дым, свет) в защищаемых помещениях;
• выдача сигналов управления на исполнительные устройства СКУД и инженерных систем {вентиляции, дымоудаления и др.) или систем пожаротушения;
• выдача сигнала и/или включение системы оповещения о пожаре;

• включение тонального или речевого оповещения о возникшей ситуации;
• ведение и архивация протокола событий состояния системы пожарной сигнализации, действий оператора, с указанием времени и даты.

Система пожарной сигнализации аналогична по структуре построения охранной сигнализации, т. е. она также состоит из различного типа извещателей и приемно-контрольных приборов. В системах пожарной сигнализации используются извещатели, реагирующие на факторы, сопровождающие возгорание (пожар): температуру, дым и свет, которые вызывают изменение состояния датчика, фиксируемое приемно-контрольным прибором.

Выбор типа и количества извещателей для защиты объекта зависит от оборудования и материалов, находящихся в защищаемом помещении. Требования по выбору их типа и количества изложены в НПБ 88-2001*. Приемно-контрольный прибор (станция) пожарной сигнализации должен обеспечивать постоянный круглосуточный контроль работоспособности извещателей и целостности линий связи (шлейфов).

Верификация (проверка) достоверности сигнала о пожаре, в комплексной системе безопасности, осуществляется с помощью системы телевизионного наблюдения. Однако, в некоторых случаях, в силу особенностей планировки, некоторые помещения могут оказаться вне зон обзора телекамер, что следует учитывать при создании системы телевизионного наблюдения.

В отличие от охранной, пожарная сигнализация во всех помещениях объекта должна постоянно находиться во включенном состоянии и контролироваться самостоятельным приемно-контрольным прибором, который, в свою очередь, подключается к интегрированной системе и может также иметь прямой выход на пожарную часть.

Система телевизионного наблюдения

Система СТН в составе КБО обеспечивает решение следующих задач:
• видеомониторинг объекта: видеоконтроль территорий вдоль ограждений и прилегающей зоны периметра, обстановки на территории и в здании, передвижения людей внутри здания, подступов к наиболее важным зонам, досмотр автотранспорта и.т.д;
• видеорегистрации состояний объекта и событий с последующим воспроизведением записанной видеоинформации;
• верификация тревожных сообщений поступивших от других систем.
В настоящее время для защиты объектов применяются различные системы видеонаблюдения, использующие аппаратуру с аналоговым, гибридным и цифровым методом обработки сигнала.

Основные преимущества цифровых систем по сравнению с традиционными аналоговыми:
• возможность длительного хранения записанной информации без потери качества;
• меньшие затраты на эксплуатационно-техническое обслуживание;
• возможность одновременной работы в режимах "записи" одного события и "воспроизведения" другого события;
• простота и надежность копирования на различные носители;
• простота и высокая скорость поиска нужного фрагмента;
• полное сохранение качества исходного материала;
• возможность применения к сигналу цифровой обработки для повышения качества подробного анализа отдельных фрагментов видеозаписей;
• возможность передачи архивных файлов по компьютерным сетям;
• возможность совмещения нескольких функций в одном устройстве {цифровой видеомагнитофон, коммутатор, детектор движения и т.д.);
• значительная гибкость и адаптивность (возможность изменять параметры системы в зависимости от конкретной задачи, стоящей перед пользователем).

Возможные варианты интеграции систем необходимо учитывать на этапе проектирования, при разработке концепции безопасности, оптимизации компоновки технических средств, топологии кабельных сетей. Использование вычислительной техники при этом позволяет:
• создавать и корректировать графические планы;
• контролировать состояние и работоспособность технических средств;
• управлять техническими средствами, используя графические планы;
• автоматически выделять на плане тревожные зоны;

• верифицировать события через ТВ систему;
• автоматически выводить на экран текстовые рекомендации, инструкции;
• фиксировать и выводить на принтер протоколы событий;
• осуществлять контроль за маршрутами патрулирования (по контрольным точкам);
• передавать информацию на центральный пульт;
• осуществлять независимую работу подсистем, входящих в комплекс.

Основные положения, в соответствии с которыми разрабатывается проект и режимы работы системы телевизионного наблюдения, определяются службой безопасности исходя из общих задач обеспечения безопасности объекта. Профессиональный подход требуется не только к отдельным элементам системы, но и ко всему комплексу в целом. Разнообразие задач, возлагаемых на каждую конкретную видеокамеру, различные условия ее эксплуатации, разница сюжетных и фоновых засветок, необходимый диапазон регулировки углов обзора и глубины резкости, необходимость автоматических или ручных настроек - все это вопросы касающиеся технических аспектов выбора телекамер.

Рассматривая современные системы телевизионного наблюдения, необходимо обратить внимание на выбор типа системы - аналоговой или цифровой. Установлено, что, начиная с некоторого уровня сложности телевизионной системы, цифровые оказываются эффективнее. Структура решения, основанная на программно-аппаратной реализации, подразумевает возможность простого изменения и дополнения функциональных возможностей системы путем несложной замены программного обеспечения. В перспективе решение, основанное на цифровых технологиях, при расширении и развитии функций системы, может привести к значительной экономии вложенных в ее создание средств.

При использовании в охране объектов телевизионных систем для визуального представления о происходящих событиях, анализа обстановки на месте происшествия, принятия решений по устранению нарушений, а также разбора ситуаций по результатам видеозаписи следует учитывать требования ГОСТ Р 51558-2000 "Системы охранные телевизионные. Общие технические требования и методы испытаний".

Использование системы телевидения в составе КСБ для наблюдения за обстановкой на объекте существенно увеличивает эффективность применения технических средств охранно-пожарной сигнализации и контроля доступа, однако особые требования при этом предъявляются к обеспечению объективности видеорегистрации. Видеонаблюдение дает также неоспоримые преимущества для принятия решений в условиях чрезвычайных ситуаций. Оператор, будучи удален от места событий, не подвергается психологическому стрессу, как непосредственные его участники, может хладнокровно и взвешенно принимать решения или выполнять заранее разработанные инструкции. Системы телевидения могут использоваться и в интересах других служб предприятия. Например, операционный контроль технологических процессов выполняет также задачи контроля качества учета и предотвращения хищений. Такое совмещение функций существенно повышает эффективность вложений в телевизионные системы.

Персонал охраны не должен иметь доступа к средствам видеорегистрации и возможности влиять на установленные в них режимы.

Информация от телевизионных камер, установленных в здании, по периметру ограждения и на территории, должна в реальном времени поступать на мониторы оперативного дежурного. Запись видеоизображений, в зависимости от требований Заказчика, осуществляется в цифровом или аналоговом виде на соответствующих устройствах записи. Существенное влияние на состав аппаратуры записи оказывает режим и время оперативного хранения записей. При наличии большого числа камер и нескольких пунктов контроля (наблюдения) для их коммутации, как правило, используются матричные коммутаторы, позволяющие осуществить вывод изображения с любой телекамеры на любой монитор пункта контроля.

Наибольшая трудность для службы охраны, при анализе обстановки по периметру, связана с повышенной вероятностью ложного срабатывания сигнализации. Сочетание системы охранной сигнализации для обнаружения нарушений на периметре с системой телевизионного наблюдения является оптимальным решением такой задачи.

Одной из проблем в системе телевизионного наблюдения, при наличии большого числа видеокамер, является разработка пульта поста наблюдения, компоновка оборудования, выбор размеров экранов мониторов и их количества, т.е. определение параметров, обусловленных психофизиологическими особенностями человека. От того, как будет решена эта задача, в значительной степени зависит

эффективность восприятия информации, правильность и скорость выработки решений в "тревожных" и критических ситуациях. Указанные вопросы должны, как правило, прорабатываться на этапе проектирования КБО, с учетом средств отображения и от других систем.

Система охранного освещения

Система охранного освещения по периметру и территории в темное время суток, а также дежурного освещения в зданиях, предназначена для создания постоянного уровня освещенности, обеспечивающего работу системы телевизионного наблюдения, возможность безопасного осмотра объектов, территории и периметра персоналом охраны. Охранное освещение обеспечивает повышение эффективности работы персонала охраны и позволяет визуально контролировать происходящие события.

При создании сети охранного освещения следует предусматривать:
• охранное освещение, постоянно включенное в темное время суток;
• "тревожное" освещение, включаемое по сигналу "тревога" от охранной сигнализации;
• аварийное освещение, включаемое при аварии охранного и/или тревожного.

Требования к энергопотреблению системы освещения, как наиболее энергоемкой, жестко связаны с возможностями источника независимого энергоснабжения. В качестве независимых источников могут использоваться малогабаритные бензо/дизельгенераторы имеющие 1,5 кратный запас по потребляемой мощности. Независимый источник охранного освещения не должен использоваться для автономного питания других (компьютерных) систем безопасности.

Охранное освещение должно:
• обеспечивать работу телевизионных камер;
• создавать необходимую равномерную освещенность охраняемой зоны;
• автоматически включаться при срабатывании охранной сигнализации периметра;
• управляться {включение/отключение) с пульта управления.

Стекла всех, устанавливаемых по периметру и территории светильников, должны быть защищены металлическими решетками.

Кабельные сети

Для подключения аппаратуры систем, как правило, используются три типа кабелей:
• кабели сигнализации;
• кабели электропитания;
• специальные кабели {коаксиальные, оптоволоконные, "витая пара" и др.). При выборе типа и способа прокладки кабеля следует учитывать особенности объекта, наличие локальной сети, трассы прокладки, требования нормативных документов, климатические и географические зоны, геологические условия и др. факторы.

Электроснабжение системы безопасности

Электропитание аппаратуры систем безопасности, установленной на объектах, как правило, осуществляется от электрических распределительных сетей общего назначения напряжением 220/380 В, частотой 50 Гц. Допустимые границы отклонения напряжения от номинального значения согласно техническим условиям на аппаратуру составляют 10-15%.
В силу целого ряда причин в электрических сетях могут происходить процессы возмущения напряжения (помехи), которые могут являться одной из причин срабатывания аппаратуры и выдачи сигнала "тревога".
Различные типы аппаратуры (извещатели, приемно-контрольные приборы, контроллеры) обладают разной степенью помехозащищенности по цепям электропитания. На объектах, сети электропитания которых подвержены таким помехам, необходимо проводить дополнительные мероприятия, направленные на повышение устойчивости работы технических средств.
Для обеспечения необходимого уровня помехозащищенности аппаратура должна удовлетворять требованиям, представленным в **таблице 1.**
Наибольшая помехозащищенность средств сигнализации, при возникновении короткого замыкания во внутренней проводке здания, достигается при ее питании непосредственно от вводно-распределительного щита. С этой целью рекомендуется использовать шины щита эвакуационного

(аварийного) освещения, а при его отсутствии - шины групповых щитов рабочего освещения.
Обеспечение электропитания технических средств систем безопасности должно соответствовать 1-ой категории надежности электроснабжения, согласно требованиям "Правил устройства электроустановок" (ПУЭ). Щит электропитания, как правило, должен устанавливаться в помещении охраны, подключаться непосредственно к щиту ввода в здание и оборудоваться средствами охранной сигнализации на открывание.
При использовании в качестве резервного источника электропитания аккумуляторных батарей или самостоятельных бензо/дизельгенераторов, помещения, где они располагаются, должны быть оборудованы в соответствии с требованиями ПУЭ (IV глава).
Резервные источники электропитания каждой системы безопасности, должны учитывать всех энергопотребителей и иметь необходимый запас по мощности.

Дополнительные технические средства

Дополнительные технические средства способствуют более оперативному реагированию на угрозы, повышают надежность их отражения и ликвидации. В качестве таких средств применяются:
• прямая внутренняя телефонная связь;
• прямая (без набора) связь с местными правоохранительными органами;
• радиосвязь между сотрудниками охраны;
• система оповещения {сеть сигнальных устройств и громкоговорителей), устанавливаемая на объекте для оповещения о каких-либо видах угроз.

Система контроля несения службы

Система СКНС в составе КБО предназначена для:
• обеспечения заданного режима движения патрульного наряда и контроля объектов, расположенных по маршруту патрулирования (обхода);
• контроля соблюдения временных графиков патрулирования;
• регистрации данных о прохождении контрольных точек на маршруте патрулирования;
• анализа и оценки эффективности работы патрульных нарядов;
• разбора нештатных ситуаций.

Система оперативной связи

Система СОС предназначена для обеспечения:
• прямой проводной связи (без набора номера) между удаленными стационарными постами охраны, периферийными пультами и центральным пультом охраны;
• прямой проводной связи (без набора номера) периферийных пультов между собой;
• прямой проводной связи (без набора номера) с точками на маршрутах патрулирования;
• по радиоканалу оперативных служебных переговоров персонала, несущего круглосуточную охрану и ответственного за безопасность объекта;
• по радиоканалу обеспечение служебных переговоров персонала, ответственного за руководство производством и ведение административно-хозяйственной деятельности;
• проводной связи с целью взаимодействия служб безопасности объектов с территориальными аварийно-спасательными службами и правоохранительными органами;
• по радиоканалу оперативное управление диспетчерскими службами в местах погрузки-выгрузки сырья и готовой продукции, технологическими процессами на производстве;
• по радиоканалу взаимодействие охранных подразделений при сопровождении грузов.
• прямой проводной связи {без набора номера) центрального пульта и узловых точек КБО для проведения планово-профилактических и эксплуатационных работ.

Система связи рассредоточенных объектов

При наличии большого количества территориально распределенных объектов требования к системе связи становятся одними из наиболее важных.

Доступ к ресурсам сети INTERNET для связи с отдаленными объектами (с высоким качеством и с минимальным временем задержки), при использовании выделенных линий связи, позволяет решать задачи соединения локальных сетей с Интернет и обменом сообщений по электронной почте. Сеть должна строится исходя из требований к единой информационно-телекоммуникационной системе.

Система СС в составе КБО обеспечивает:
• связь между центральным и периферийными пультами охраны;
• связь между системами КСБ;
• связь с заинтересованными ведомствами;
• интеграцию, т.е. совмещение всех видов информации в стандартных форматах;
• использование информации в реальных масштабах времени;
• максимальное использование ведомственных линий связи и минимизацию использования арендованных линий;
• возможность реконструкции и модернизации системы без нарушения функционирования.

Указанные выше особенности систем связи для территориально рассредоточенных объектов должны учитываться при организации каналов связи. Использование каналов, не соответствующих нужным параметрам, может свести на нет усилия по охране объектов.

Приложение 4

Классификация объектов по группам защиты (Р 78,36,003-99)

Группа Защиты	Степень защиты от проникновения	Организация охранной сигнализации	
1	Недостаточная	Блокировка только отдельных участков (дверей, окон, стен и т.д.) периметра (1 рубежа) помещения	3 и 4 категории, ра группу защиты от
2	Средняя	Блокировка периметра (1 рубежа) помещения, блокировка объема (2 рубежа) помещения	3 категории , распо 2 катего
3	Высокая	Блокировка периметра (1 рубежа) и объема (2 рубежа) помещения	1 катего
4	Очень высокая	Блокировка периметра (1 рубежа), объема (2 рубежа) и самих материальных ценностей или подходов к ним (3 рубежа) охраняемого помещения	2 категории, ра

Приложение 5

Влияние помех на функционирование датчиков

Виды и источники помех	
	Ударно и магнит контактные
Внешние акустические помехи и шумы, создаваемые вблизи объекта транспортными средствами, строительными машинами и агрегатами, летательными аппаратами, погрузочными и разгрузочными работами и т.п.	Не влияют
Внутренние акустические помехи и шумы, создаваемые на объекте холодильными установками, вентиляторами, телефонными и электрическими звонками, дросселями люминесцентных ламп, гидравлическими шумами в трубах	Не влияют

Виды и источники помех			
	Ударно и магнитоконтактные	Ультразвуковые	Пас зву
Совместная работа в одном помещении извещателей одного принципа действия	Не влияет	Правильно установить и настроить извещатель	Не
Вибрация конструкций	При н		
Движущиеся предметы и люди за некапитальными стенами, деревянными дверями	Не влияют		
Движущиеся предметы в охраняемой зоне: наличие штор, растений, вращение лопастей вентиляторов	Не влияют	Не устанавливать вблизи источника помех. Правильно настроить извещатель	Не
Мелкие животные (мыши, крысы)	Не влияют	Правильно установить и настроить извещатель	Не
Движение воды в пластмассовых трубах	Не влияет	Не устанавливать вблизи источника п Правильно настроить извещател	
Изменение свободного пространства охраняемой зоны за счет внесения или вынесения крупногабаритных предметов, обладающих повышенной способностью поглощения или отражения	Не влияет		
Колебания напряжения в сети переменного тока			
Электромагнитные помехи, создаваемые: транспортными средствами с электродвигателями, мощными радиопередатчиками, электросварочными аппаратами, линиями электропередач, электроустановками мощностью более 15 кВА	Не влияют	При напряженнос	
Люминесцентное освещение	Не влияет		
Изменение температуры фона	Не вл		
Засветка светом солнца, фар транспортных средств	Не вл		

Система контроля и управления доступом (СКУД)

Система контроля прохода (СКП)

Для обоснования применения и качественной разработки СКУД необходимо иметь нормативные документы, а также справочную литературу по вопросам выбора и применения СКУД и СКП.
Система контроля и управления доступом - одно из направлений технических средств обеспечения безопасности. В рабочее время система охранной сигнализации обычно отключена, и контроль за помещениями, сотрудниками и посетителями в это время можно возложить на СКУД. В то же время, сотрудники, обладающие необходимыми полномочиями, свободно могут перемещаться по объекту.
Система контроля прохода - это комплекс организационно-технических мероприятий по организации пропуска (входа и выхода) работников предприятия, ведения учета, создания необходимой базы данных.
Терминология СКП, как правило, аналогична понятиям, принятым для СКУД.
Прежде чем рассматривать СКУД и СКП, необходимо остановиться на некоторых терминах и определениях, используемых в данной области.

Термины и определения понятий по средствам и системам контроля и управления доступом

• ***Доступ*** - перемещение людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.
• ***Несанкционированный доступ*** - доступ людей или объектов, не имеющих права доступа.
• ***Санкционированный доступ*** - доступ людей или объектов, имеющих права доступа.
• ***Контроль и управление доступом (КУД***) - комплекс мероприятий, направленных на ограничение и санкционирование доступа люден, транспорта и других объектов в (из) помещения, здания, зоны и территории.
• ***Средства контроля и управления доступом (средства КУД)*** - механические, электромеханические, электрические, электронные устройства, конструкции и программные средства, обеспечивающие реализацию контроля и управления доступом.
• ***Система контроля и управления доступом (СКУД)*** - совокупность средств контроля и управления, обладающих технической, информационной, программной и эксплуатационной совместимостью.
• ***Идентификация*** - процесс опознавания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку. Под идентификацией понимается также присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
• ***Биометрическая идентификация*** - идентификация, основанная на использовании индивидуальных физических признаков человека.
• ***Идентификатор доступа, идентификатор (носитель идентификационного признака)*** - уникальный признак субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код. биометрический признак иди вещественный код.
• ***Идентификатор, использующий вещественный код*** - предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и т.д.).
• ***Вещественный код*** - код. записанный на физическом носителе (идентификаторе).
• ***Запоминаемый код*** - код, вводимый вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств.
• ***Устройства преграждающие управляемые (УПУ)*** - устройства, обеспечивающие физическое препятствие доступу людей, транспорта и других объектов и оборудованные исполнительными устройствами для управления их состоянием (двери, ворота, турникеты, шлюзы, проходные кабины и т.п. конструкции).
• ***Устройства исполнительные*** - устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние УПУ (электромеханические и электромагнитные замки, защелки, механизмы привода шлюзов, ворот, турникетов и т.д.).
• ***Устройства ввода идентификационных признаков (УВИП)*** - электронные устройства, предназначенные для ввода запоминаемого кода, ввода биометрической информации, считывания кодовой информации с идентификаторов. В состав УВИП входят считыватели и идентификаторы.
• ***Считыватель*** - устройство в составе УВИП. предназначенное для считывания (ввода) идентификационных признаков.
• ***Устройства управления (УУ)*** - устройства и программные средства, устанавливающие режим доступа и обеспечивающие прием и обработку информации с УВИП. управление УПУ. отображение и регистрацию информации.
• ***Точка доступа*** - место, где непосредственно осуществляется контроль доступа (например, дверь, турникет, кабина прохода, оборудованные считывателем, исполнительным механизмом.

электромеханическим замком и другими необходимыми средствами).
• ***Зона доступа*** - совокупность точек доступа, связанных общим местоположением или другими характеристиками (например, точки доступа, расположенные на одном этаже).
• ***Временной интервал доступа (окно времени)*** - интервал времени, в течение которого разрешается перемещение в данной точке доступа.
• ***Уровень доступа*** - совокупность временных интервалов доступа (окон времени) и точек доступа, которые назначаются определенному лицу или группе лиц, имеющим доступ в заданные точки доступа в заданные временные интервалы.
• ***Правило двух (и более) лиц*** - правило доступа, при котором доступ разрешен только при одновременном присутствии двух или более людей.
• ***Пропускная способность*** - способность средства или системы КУД пропускать определенное количество людей, транспортных средств и т.п. в единицу времени.
• ***Несанкционированные действия (НСД)*** - действия, целью которых является несанкционированное проникновение через УПУ.
• ***Взлом*** - действия, направленные на несанкционированное разрушение конструкции.
• ***Вскрытие*** - действия, направленные на несанкционированное проникновение через УПУ без его разрушения.
• ***Манипулирование*** - действия, производимые с устройствами контроля доступа без их разрушения, целью которых является получение действующего кода или приведение в открытое состояние заграждающего устройства. Устройства контроля доступа могут при этом продолжать правильно функционировать во время манипулирования и после него; следы такого действия не будут заметны. Манипулирование включает в себя также действия над программным обеспечением.
• ***Наблюдение*** - действия, производимые с устройствами контроля и управления доступом без прямого доступа к ним, целью которых является получение действующего кода.
• ***Копирование*** - действия, производимые с идентификаторами, целью которых является получение копии идентификатора с действующим кодом.
• ***Принуждение*** - насильственные действия над лицом, имеющим право доступа, с целью несанкционированного проникновения через УПУ. Устройства контроля и управления доступом при этом могут функционировать нормально.
• ***Саботаж (состояние саботажа)*** - преднамеренно созданное состояние системы, при котором происходит повреждение части системы.
• ***Устойчивость к взлому*** - способность конструкции противостоять разрушающему воздействию без использования инструментов, а также с помощью ручных и других типов инструментов.
• ***Пулестойкость*** - способность преграды противостоять сквозному пробиванию пулями и отсутствие при этом опасных для человека вторичных поражающих элементов.
• ***Устойчивость к взрыву*** - способность конструкции противостоять разрушающему действию взрывчатых веществ.

Контроль и управление доступом - это комплекс мероприятий, направленных на ограничение и санкционированное передвижение людей и средств, перемещение предметов в помещениях, зданиях сооружениях и на территории объектов. Технические средства включают в себя механические, электромеханические, электрические конструкции, устройства и программные средства, обеспечивающие реализацию контроля и управления доступом. В основу функционирования СКУД положен принцип сравнения тех или иных идентификационных признаков принадлежащих конкретному физическому лицу или объекту и заложенных в память системы.

Кроме своих непосредственных задач. СКУД обеспечивает:
- сбор и обработку информации о перемещениях лиц и предметов по объекту;
- организацию и учет рабочего времени;
- управление освещением, лифтами и автоматикой объекта;
- прием команд от охранно-пожарной сигнализации;
- управление приборами ТСН.

При решении собственных задач СКУД должна выполнять следующие функции:
• ***санкционирование*** - присвоение каждому пользователю персонального идентификатора, регистрацию его в СКУД и задание временных интервалов и уровня доступа для пользователя (в какие помещения и когда он имеет право прохода);
• ***идентификация*** - опознание пользователя по предъявляемому идентификатору;
• ***аутентификация*** - установление подлинности пользователя по предъявленному идентификатору;
• ***авторизация*** - проверка полномочий, установленных в процессе санкционирования:
• ***разрешение доступа и отказ в доступе*** - анализ результатов предыдущих процедур;
• ***регистрация*** - протоколирование всех действий в СКУД;

• ***реагирование*** - реакция СКУД на несанкционированные действия (подача предупреждающих и тревожных сигналов, отказ в доступе и т.л.).

Санкционирование осуществляется оператором или администратором СКУД и заключается во вводе необходимых данных в компьютер СКУД или в контроллер. Все остальные функции СКУД выполняются автоматически.
Понятия ***идентификатор и идентификация*** являются основными для СКУД. Одной из важных характеристик СКУД является ее структура. По структуре СКУД разделяются на два основных вида:
- ***автономная*** - для управления одним или несколькими заграждающими устройствами, без передачи информации на центральный пульт охраны и без контроля со стороны дежурного оператора;
- ***сетевая*** - для управления большим количеством заграждающих устройств, с обменом информацией с центральным пультом и возможностью контроля и управления СКУД со стороны дежурного оператора.

С точки зрения усиления режима обеспечения безопасности объекта, интерес представляет интегрирование СКУД с системами СОС и СТН. Говоря об интеграции этих систем, следует выделить два наиболее общих уровня - интеграция на релейном и на системном уровнях.
Репейный уровень предполагает наличие дополнительного модуля (или дополнительных входов/выходов) в контроллере, к которому подключаются охранные или пожарные извещатели и релейные выходы для управления телекамерами и другими устройствами.
Системный уровень предполагает подключение к общей магистральной линии (каналу связи, сети) отдельных контроллеров (охранные панели, контроллеры управления СТН).
Интеграция с СТН на системном уровне предполагает управление телекамерами с выводом изображения в реальном масштабе времени на экран монитора. Такая интеграция должна поддерживаться соответствующим программным обеспечением.

Системы СКУД и СКП в составе КСБ предназначены для:
• регламентации доступа в пространственные и временные зоны объекта;
• блокирования в зоне прохода нарушителей пропускного режима:
• блокирования выхода из зоны в случае поступления сигнала тревоги или попытки несанкционированного прохода;
• формирования и архивации данных о том кто, когда был допущен и на каком временном интервале находился в установленных зонах доступа или делал попытки прохода;
• совместной работы с системой охранно-тревожной сигнализации и видеонаблюдения;
• управления исполнительными устройствами: турникетами, замками, шлюзами, шлагбаумами.

Для обеспечения доступа сотрудников в различные объекты (подразделения) используются карты-пропуска. Карты-пропуска в полном объеме определяют статус пользователя, территориально-пространственные и временные зоны доступа. С помощью персональной карточки-пропуска обеспечивается доступ во все разрешенные помещения, а также возможность "сдачи-снятия" соответствующих помещений с охраны. При перемещении персонала внутри объекта и для прохода в рабочие помещения, защищенные системами автоматизированного доступа, также используются личные карточки-пропуска.

Структурная схема системы управления доступом в различные зоны или помещения реализуется по сетевому принципу. Каждой зоне или помещению в программе присваивается определенный статус, в соответствии с которым сотрудники имеют право входа/выхода в ту или иную зону, однако в целом система представляет собой единый аппаратно-программный комплекс.

Контролируемые СКП и СКУД элементы объекта:
• входы (въезды) на объект;
• внутренние зоны и помещения;
• специальные зоны и помещения;
• зоны и помещения свободного доступа.
• ***Вход (въезд) на объект*** - зона (КПП), через которую осуществляется централизованный контроль и учет входящих/выходящих сотрудников и посетителей (транспорта) в соответствии с установленным графиком.
• ***Внутренние зоны и помещения*** - элементы объекта, для которых необходимо разграничение доступа, но ведение протокола прохода пользователей не является необходимым (рабочие помещения, помещения, уровень доступа в которые может быть изменен в течение рабочего дня и т.п.).
• ***Специальные зоны и помещения ограниченного доступа*** - элементы объекта, для которых производится разграничение доступа и необходимо ведение протокола прохода пользователей (кабинеты руководства, помещения с материальными ценностями, серверные, кассовые узлы, складские

помещения с вредными и ядовитыми веществами, АТС и т.п.).
• ***Помещения и зоны свободного доступа*** - здесь не рассматриваются.

Организация доступа на объект

Лица, посещающие объект или его отдельные помещения, подразделяются на следующие категории:
• персонал;
• постоянные посетители;<
• разовые посетители;
• злоумышленники.

Доступ персонала и посетителей на территорию объекта и в служебные помещения может осуществляться:
• с выдачей постоянного электронного пропуска;
• с выдачей разового электронного пропуска;
• с выдачей временного электронного пропуска в конкретную зону или помещение.

Вопрос возврата разовых и временных пропусков решается организационно-техническими мероприятиями.

В состав СКУД и СКП входят:
- "основные элементы": контроллеры, исполнительные механизмы и считыватели,
- "дополнительные элементы": дверные доводчики, аудио- и видеодомофоны, резервное питание, металлодетекторы, устройства дистанционного отпирания дверей и др.)
Контролируемое ограничение прохода (доступа) достигается использованием турникетов, замков и защелок электромагнитных или электромеханических, а также шлюзовых кабин.

Защита от несанкционированного доступа

Установление режима контроля прохода на объект подразумевает создание рубежей контроля на пути следования персонала и определения порядка его прохода через рубежи контроля с целью выявления и блокирования попыток проникновения злоумышленников.
Следует учитывать, что статус субъекта контроля может изменяться в зависимости оттого, какой рубеж контроля он пытается преодолеть. Например, сотрудник, пытающийся зайти в помещение, доступ в которое ему запрещен, автоматически превращается в потенциального злоумышленника.
Для обеспечения доступа персонала и постоянных посетителей целесообразно выдавать им персональные карточки-пропуска (идентификаторы), а постоянным и разовым посетителям - персональные пропуска с ограниченным сроком действия.
Организация прохода людей на территорию объекта влечет за собой одновременное решение целого ряда вопросов. В первую очередь, к ним относятся безопасность персонала и посетителей, сохранность материальных ценностей и информации, кадровый и бухгалтерский учет, трудовая дисциплина и т.д.
Особое внимание должно уделяться системе прохода (СКП) на объект при большом количестве сотрудников (более 5 000 человек), различных режимах работы, как предприятия, так и его подразделений. Компоненты, входящие в систему, должны обеспечивать надежную и бесперебойную работу устройств контроля прохода наряду с обработкой и регистрацией данных по потоку сотрудников.
Обработка в СКП производится с помощью ЭВМ. Базовый вариант включает в себя сервер системы, программу конфигурации, программу управления, программу "отдел кадров", генератор отчетов, программу администратора системы. Кроме этого, возможно расширение возможностей системы за счет развития программного обеспечения такими блоками программ, как учет рабочего времени, создание архива, оформление пропусков, управление инженерными средствами (турникетами, шлагбаумами, видеокамерами и т.п.)

Доступ во внутренние зоны и помещения.

Технические средства идентификации

Для обеспечения входа на объект, а также прохода в помещения, оборудованные системой контроля доступа, персоналом используются электронные идентификаторы (карточки-пропуска).
К положительным характеристикам таких средств следует отнести:
- скрытность записанного кода и самого процесса идентификации (нет необходимости набирать кодовые комбинации на клавиатуре);

- простоту процесса считывания;
- возможность интеграции со средствами обеспечения безопасности компьютерных систем и другими приложениями по технологии единого ключа.

При необходимости организации централизованного прохода на предприятие более 5000 человек или/и при рассредоточенных зонах ограниченного доступа, целесообразно систему контроля доступа для нескольких помещений (зон), выделить из системы контроля прохода и интегрировать ее с системой охранной сигнализации. Такой подход вызван тем, что организация ограничения доступа, как правило, связана с необходимостью персонального взятия (снятия) с охраны объектов (зон) конкретными сотрудниками.

Для особо важных помещений возможна организация более сложных постов контроля доступа:
• карта + персональный пин-код на дополнительной клавиатуре;
• подтверждение права доступа второй картой;
• одновременное предъявление двух карт;
• с подтверждением права доступ а оператором системы после сравнения им видеоизображения владельца карты или отпечатков пальцев (биометрические считыватели) с эталонным из базы данных системы и т.п.

Выход персонала из таких помещений происходит аналогично входу или с использованием кнопки, открывающей замок.
По окончании рабочего дня персонал с помощью карточек-пропусков сдает помещения под охрану, после чего замки их дверей блокируются системой.
Возможности оснащения объектов системой контроля доступа и мероприятия, необходимые для обеспечения функционирования системы приведены в таблице 2.

Таблица 2. Возможности оснащения объектов системой контроля доступа и мероприятия, необходимые для обеспечения функционирования системы

Виды и источники помех			
	Ударно и магнитоконтактные	Ультразвуковые	Пас зву
Совместная работа в одном помещении извещателей одного принципа действия	Не влияет	Правильно установить и настроить извещатель	Не
Вибрация конструкций	При н		
Движущиеся предметы и люди за некапитальными стенами, деревянными дверями	Не влияют		
Движущиеся предметы в охраняемой зоне: наличие штор, растений, вращение лопастей вентиляторов	Не влияют	Не устанавливать вблизи источника помех. Правильно настроить извещатель	Не
Мелкие животные (мыши, крысы)	Не влияют	Правильно установить и настроить извещатель	Не
Движение воды в пластмассовых трубах	Не влияет	Не устанавливать вблизи источника п Правильно настроить извещател	
Изменение свободного пространства охраняемой зоны за счет внесения или вынесения крупногабаритных предметов, обладающих повышенной способностью поглощения или отражения	Не влияет		
Колебания напряжения в сети переменного тока			
Электромагнитные помехи, создаваемые: транспортными средствами с электродвигателями, мощными радиопередатчиками, электросварочными аппаратами, линиями электропередач, электроустановками мощностью более 15 кВА	Не влияют	При напряженнос	
Люминесцентное освещение	Не влияет		
Изменение температуры фона	Не вл		
Засветка светом солнца, фар транспортных средств	Не вл		

Функционирование систем

После установки СКП и СКУД производится регистрация каждого пользователя, т.е. в базу данных вводится фамилия, номер идентификатора, а также устанавливаются полномочия по доступу в отдельные помещения.
В процессе работы система автоматически ведет протокол событий с записью даты и времени прохода или попытки несанкционированного прохода.
На основании анализа протоколов событий возможно производить учет посещаемости, рабочего времени, выявление лиц, пытавшихся нарушить режим прохода, а также составлять различные отчеты по посещению объекта.

Система фиксации номеров автотранспорта

Схема фиксации номеров автотранспорта выполняется на базе специализированной телевизионной системы, обеспечивающей идентификацию даже загрязненных госномеров автомашин.
Система СФНА в составе КСБ решает следующие основные задачи:
• регламентация доступа в пространственные и временные зоны объекта;
• формирование и архивация данных о количестве и гос. номерах автомашин, которые въезжали/выезжали из установленных зон доступа;
• совместная работа с системой видеонаблюдения;
• управление исполнительными устройствами контроля въезда/выезда (шлюзами, шлагбаумами и др.);
• регистрировать и автоматически вести учет автотранспорта;
• использовать для въезда/выезда идентификационные карты-пропуска;
• вести протокол и формировать базы данных;
• иметь возможность наращивания системы при увеличении точек контроля. Важнейшей отличительной особенностью автоматической системы фиксации номеров автотранспорта является возможность жесткого контроля над въезжающим/выезжающим транспортом и исключение "человеческого" фактора.

Специфика организации службы охраны

Эффективность оснащения объекта комплексом технических средств охраны может быть сведена к нулю неквалифицированными действиями персонала охраны.
Служба охраны организуется и осуществляет свою деятельность в соответствии с разработанными и утвержденными руководством объекта внутренними нормативными документами. К их числу относятся инструкции о пропускном и внутриобъектовом режимах, порядке реагирования на сигналы тревоги, организации эксплуатационного обслуживания и т.п. документы, в которых изложены задачи, права и обязанности сотрудников службы охраны.

Категории персонала охраны

На объекте обычно заняты следующие категории персонала с соответствующими обязанностями:

1. Операторы, находящиеся в пультовом зале, наблюдающие за индикаторами сигналов тревоги и предупреждающие других сотрудников об инцидентах, требующих внимания.
Нормальный, специально не тренированный оператор может воспринимать поступающую информацию не более чем по 5-6 информационным направлениям, а оперативно реагировать только по одному. Выбор этого одного направления подчас не бывает самым правильным, что в ситуациях с жестко ограниченными временными интервалами приводит к неадекватной реакции оператора на произошедшее событие и, как следствие, к трудно предсказуемым последствиям. Недопустимо вменять этой группе сотрудников выполнение во время дежурства других функций.
2. Дежурные, несущие службу на охраняемых площадках, проходных и т.п. В их обязанность входит сообщить оперативному дежурному об изменении ситуации и об инцидентах, не покидая охраняемой площади. Этой категории лиц может быть вменено в полномочия отражать нападение нарушителей.
3. **Сотрудники оперативной (дежурной) группы** подразделения охраны используются для решения разнообразных задач: от физического вмешательства в инцидент и задержания нападающих до расследования обстоятельств нарушения.
4. Сотрудники эксплуатационной группы используются для эксплуатационно-технического обслуживания технических средств установленных систем.

Действия службы охраны

Действия группы реагирования будут эффективны только тогда, когда будут обеспечены следующие необходимые условия:
■ вдоль охраняемого периметрального рубежа (с внутренней стороны) или к охраняемым на территории объектам должна быть проложена дорога с твердым покрытием (как минимум гравийная) для проезда транспорта группы к месту срабатывания сигнализации; зимой дорога должна вовремя расчищаться;
■ охраняемая зона и пути возможного движения нарушителя должны быть освещены;
■ группа реагирования должна быть оснащена средствами защиты и задержания, оружием, спецсредствами, средствами связи, обеспечивающими устойчивую связь в любой точке объекта;
■ автомобиль (желательно повышенной проходимости) зимой должен находиться в утепленном гараже, в максимальной готовности.

На больших по протяженности периметрах организуются две и более групп реагирования (подвижных нарядов), чтобы обеспечивалось безусловное опережение действий нарушителя. На таких объектах желательно организовать периодические объезды или обходы охраняемого рубежа, территории, объекта. Для контроля за периодичностью обхода (осмотра) могут использоваться специальные приборы контроля несения службы (КНС) установленные на маршруте патрулирования. Для связи с центральным пультом должна использоваться система оперативной радиосвязи или проводная система (без набора номера).

Центральный пункт охраны

Центральный пункт охраны в комплексе технических средств охраны объекта, занимает главное место. Сюда сводится вся информация от средств сигнализации и теленаблюдения, здесь анализируются сигналы "тревога" и принимаются решения по оперативному реагированию, отсюда организуется централизованное электроснабжение и управление освещением охранной зоны, контролируются источники гарантийного электроснабжения и т.д. Обычно здесь же находится группа реагирования. В связи с этим необходимо обеспечить надлежащие психофизиологические условия работы персонала и выполнение требований эргономики.

Информацию от средств сигнализации обычно получает дежурный оператор, дальнейшие действия которого определяются должностной инструкцией. На больших объектах за пультом могут также находиться оперативный дежурный, помощник начальника караула (или сам начальник), которые могут своевременно принять решения по поступающим сигналам.

Выбор вариантов оборудования для построения центрального пульта управления КСБ определяется следующими критериями:
■ функциональная достаточность: каждый из элементов системы должен иметь технические характеристики, достаточные для выполнения возложенных на него функций в системе, с соответствующими механизмами реагирования;
■ надежность в работе в условиях, характерных для данного объекта;
■ соотношение надежность/ цена/ качество для элементов системы и для КСБ в целом;
■ возможность перспективного развития системы и ее гибкость, по отношению к изменениям в структуре системы безопасности.

Для обеспечения оперативного управления, координации действий и передачи информации сотрудникам охраны на центральном пункте обычно устанавливается несколько видов связи:
■ постовая телефонная - для прямой связи постов между собой и с центральным пунктом;
■ радиосвязь - для радиосвязи стационарной станции с носимыми станциями подвижных групп;
■ городская телефонная - для вызова аварийных и правоохранительных и других служб (снабженная аппаратурой автоматического определения номера и записи переговоров).

Очень важно, чтобы информация от средств сигнализации, в первую очередь тревожная, не пропала из-за неумелых действий дежурного оператора. Поэтому одной из функций КСБ должно быть автоматическое документирование всех событий с указанием их видов, привязкой к месту (номерами участков, помещений или зон и т.п.) и времени (дата, часы, минуты), а также документирование действий оператора. Это позволяет организовать не только контроль за работой техники и персонала, но и практически исключить возможность сговора с нарушителями.

Организация автоматической передачи тревожной информации на более высокий управленческий уровень и ее документирование способствуют повышению уровня исполнительской дисциплины работников охраны.

Действия оперативного дежурного будут более осмысленными и эффективными если на экран монитора будет выводиться схема объекта с указанием участка или датчика, вызвавшего тревогу.
Личный состав оперативной группы реагирования должен быть обучен действовать на опережение, владеть искусством поиска, грамотно задерживать и обыскивать нарушителя, изымать оружие и т.п. Группа реагирования должна быть готова к тому, что нарушители могут организовать засады и предусмотреть контрмеры. Личный состав должен хорошо владеть штатным вооружением, спецсредствами, приборами ночного видения и т.п. аппаратурой.

Техническое обслуживание

Техническое обслуживание есть совокупность организационно-технических мероприятий обеспечивающих поддержание в исправном состоянии и восстановление работоспособности технических средств систем безопасности.

Техническое обслуживание включает в себя:
■ планирование технического обслуживания;
■ подготовку и допуск личного состава охраны (или эксплуатационного подразделения) к техническому обслуживанию;
■ техническое обслуживание;
■ ремонт технических средств;
■ приемку технических средств по комплектности, при приемке в эксплуатацию;
■ метрологическое и инструментальное обеспечение обслуживания;
■ соблюдение техники безопасности при обслуживании;
■ эксплуатационный контроль технических средств;
■ сбор и обобщение информации о техническом обслуживании;
■ ведение эксплуатационной документации;
■ материально-техническое обеспечение технического обслуживания.

Планирование технического обслуживания

Целью планирования технического обслуживания средств сигнализации является обеспечение организации и своевременного проведения мероприятий, направленных на эффективное использование, поддержание в исправном состоянии и восстановлении технических средств.
Планирование технического обслуживания осуществляется на основании:
■ издаваемых приказов и указаний по подразделению охраны;
■ анализа состояния работ по техническому обслуживанию;
■ анализа надежности охраны объекта с помощью технических средств.

Нормы обслуживания технических средств

Нормы обслуживания технических средств устанавливаются на основании времени необходимого на:
■ проверку технического состояния и ремонт имеющихся технических средств;
■ сроков службы технических средств;
■ норм положенности средств измерений, инструмента, запасных частей и материалов.

Техническое обслуживание систем комплекса проводится периодически по установленной форме. В процессе обслуживания проверяется общая работоспособность систем и комплекса в целом.
Техническое обслуживание - один из важных этапов в создании и функционировании КСБ. Подготовкой кадров в этой области должны заниматься высококвалифицированные профессионалы. Начало такой работы может быть положено на этапе пуско-наладки систем КСБ. Дальнейшее обучение, как теоретическое, так и практическое может быть продолжено на этапе технологического "прогона" аппаратуры.
Одной из основных задач при внедрении КСБ в охрану объектов является создание в подразделении охраны эксплуатационно-технической службы (или подготовка специалиста) для обслуживания установленной аппаратуры. В случае невозможности проведения ТО техническими специалистами службы охраны **целесообразно** проводить ТО силами сторонних монтажных организаций, имеющих соответствующие лицензии с учетом регионального представительства.

Основными задачами технического обслуживания являются:
■ обеспечение устойчивого функционирования технических средств (ТС);
■ контроль технического состояния ТС;

■ выявление, анализ и устранение неисправностей и причин ложных тревог;
■ ликвидация последствий воздействия на ТС климатических, технологических и иных неблагоприятных условий;
■ анализ и обобщение данных по результатам выполнения работ, разработка мероприятий по совершенствованию технического обслуживания;
■ текущий ремонт аппаратуры.

Планирование технического обслуживания осуществляется с учетом количества аппаратуры, установленной на каждом объекте.

Сбор и обобщение информации по технической эксплуатации

Сбор и обобщение информации производится с целью получения дополнительных данных для разработки организационно-технических мероприятий по совершенствованию технического обслуживания, ремонта, улучшения эксплуатационных характеристик и уменьшения ложных срабатываний.

Задачами сбора и обобщения информации является:
■ накопление статистических данных по срабатываниям и причинам неисправностей технических средств;<
■ оценка правильности выбора технических средств для конкретных условий эксплуатации;
■ накопление данных по выявленным неисправностям в процессе ремонта и проверки технического состояния.

Первичным источником информации по технической эксплуатации является ежесуточная распечатка информации обо всех сигналах, поступивших на центральный пульт от систем безопасности, установленных на объекте. Все распечатки, с момента начала эксплуатации, должны храниться в отдельной папке наравне со служебной документацией.
Для эксплуатационного обслуживания технических средств требуется обслуживающий персонал соответствующей квалификации. Главное условие качественной работы технических средств - аккуратность, своевременность обслуживания, четкое соблюдение нормативной и эксплуатационной документации.

Эксплуатационно-техническое обслуживание организуется в соответствии с:
■ эксплуатационной документацией на оборудование;
■ требованиями нормативной документации;
■ проектно-исполнительской документацией;
■ ведомственными инструкциями, составленными для конкретного объекта.

С учетом имеющихся потребностей, перспективных планов и других факторов администрации предприятия и руководству службы безопасности необходимо также иметь в виду, что внедрение в охрану объектов комплексной системы безопасности повлечет за собой и структурные изменения в расстановке кадров. Уровень этих изменений будет зависеть от того, насколько полно будут учтен весь объем вопросов, связанных с оснащением объекта комплексной системой безопасности.

Ложные тревоги

Ложные тревоги - это срабатывания средств сигнализации, вызванные сбоями (отказами) аппаратуры или линий связи или другими событиями, не связанными с попытками проникновения нарушителей на охраняемые объекты, в результате которых на центральный пульт поступают тревожные сообщения. Главным показателем надлежащего уровня эксплуатационно-технического обслуживания является количество ложных срабатываний (тревог) технических средств. Для предотвращения ложных тревог не следует упрощать смысл их определения и человеческого фактора. В этом контексте система состоит из окружающей среды, пользователя, коммуникаций, оборудования и службы охраны.
Для полного понимания проблемы нужно рассмотреть все источники ложных тревог, т.к. игнорирование любого из них может привести к значительному убытку. Профилактика ложных тревог начинается с грамотно установленных извещателей охранной сигнализации. В этих целях на этапе согласования проектной документации целесообразно обратиться к данным, приведенным в **Приложении 5**, т.к. игнорирование внешних факторов может стать впоследствии серьезной проблемой.
Простого статистического выражения эффективности предотвращения преступлений - не существует. Более полное представление дает сравнение количества ложных тревог со временем, в течение

которого они зарегистрированы. Этот показатель, как правило, является критерием качества эксплуатационного обслуживания и работы персонала.
Возможности КСБ позволяют вести и ежедневно получать распечатку всех, поступивших от систем сигналов, в т.ч. ложных. Проведение анализа всех тревог по объектам (номерам), времени и другим закономерностям, позволяет своевременно принять действенные меры к выявлению причин их вызвавших и соответственно к сокращению, а также к повышению надежности работы систем.
Отсутствие должного внимания к этому участку работы приводит к довольно ощутимым отрицательным последствиям: охрана перестает реагировать на повторяющиеся сигналы "тревога", что чревато пропуском реального сигнала "тревога".