СИСТЕМНАЯ КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ

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

В данной работе излагаются основные направления деятельности по обеспечению безопасности объектов охраны, привлекательных для преступников с различных точек зрения. Преступные посягательства могут преследовать различные цели, например:

- кражи материальных и/или информационных ценностей;

- имеющие в своей основе террористические действия, направленные на решение политических или грабительских задач, как то: разрушение объекта; захват управления функционированием объекта; информационная разведка; ограбление; внедрение членов организованных преступных формирований или групп в управленческие структуры и т.д.

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

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

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

- по данным экспертов подготовка и проведение преступных акций в большинстве случаев осуществляются на высоком профессиональном уровне, характеризуются системным решением и часто отличаются жестокостью исполнения.

Исходя из изложенного, разработчики системной концепции обеспечения безопасности объектов в максимальной степени должны учитывать мировой и отечественный опыт, касающийся всей многогранной деятельности, организуемой по защите объектов.

Практика охранной деятельности показывает, что необходим научно обоснованный подход к решению проблем и задач охраны объектов, в особенности, если это особо важные, особо опасные объекты, объекты особого риска или объекты, содержащие большие материальные ценности.

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

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

Технические средства охраны, установленные на объектах охраны, должны в комплексе с силами физической охраны и системой инженерных сооружений удовлетворять современным требованиям по охране 00 от устремлений потенциального нарушителя.

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

- наличие в свободной продаже зарубежных и отечественных изделий спецтехники;

- возможность приобретения современного вооружения;

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

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

Одной из центральных подсистем в системе обеспечения безопасности 00 является автоматизированная система охраны, с помощью которой реализуются практические меры по предупреждению недозволенного доступа к технике, оборудованию, материалам, документам и охране их от шпионажа в пользу конкурентов, диверсий, повреждений, хищений и других незаконных или преступных действий.

На практике действия АСО складываются из двух основных фаз: обнаружение нарушителя и его задержание.

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



Рис.1.1 Структура автоматизированной системы охраны

В общем случае в состав комплекса технических средств обеспечения безопасности объекта входят: технические средства охранной сигнализации; технические средства наблюдения; система контроля доступа, в литературе применяются также понятия-синонимы — система управления доступом и система контроля и управления доступом; технические средства пожарной сигнализации; технические средства обнаружения диверсионно-террористических средств и технические средства обнаружения утечки информации. В состав ТСОС входят: средства обнаружения; система сбора, обработки, отображения и документирования информации; вспомогательные устройства - системы электропитания, охранного освещения, оповещения и т.д.

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

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

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

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

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

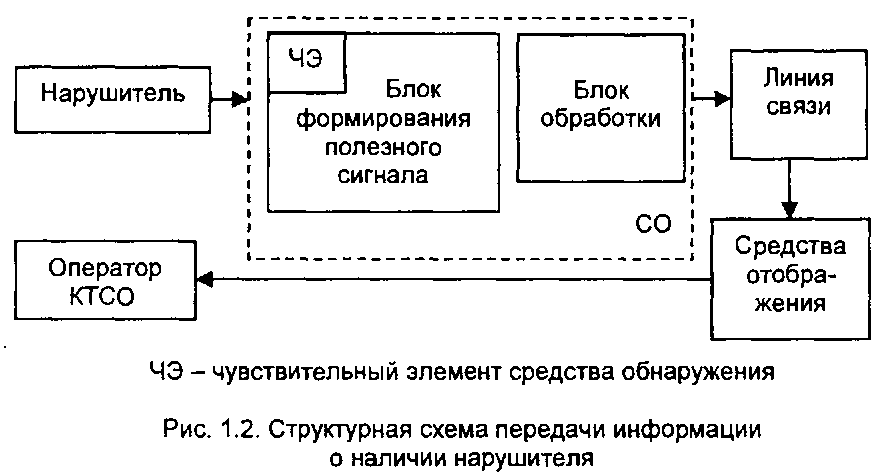
- нарушитель имеет доступ на объект, в режимную зону и к конкретным охраняемым сведениям или материальным ценностям.

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

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

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

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



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

Вероятность обезвреживания нарушителя силами физической охраны существенно зависит от характеристик ТСОС. Первая фаза - обнаружение нарушителя - определяется вероятностью обнаружения нарушителя ТСОС, периодом наработки на отказ и временем восстановления ТСОС; вторая фаза - задержание нарушителя - зависит от времени обнаружения нарушителя техническими средствами охранной сигнализации с момента его появления на объекте и периода наработки на ложное срабатывание. Последнее объясняется тем, что при ложном срабатывании силы физической охраны отвлекаются на время проверки сигнала "Тревога" и не способны провести проверку двух и более фактов сработки ТСОС одновременно. Кроме того, ложное срабатывание создает с неизбежностью стрессовую ситуацию, снижающую боеготовность сотрудников сил физической охраны на некоторый период времени, необходимый для восстановления гормонального баланса человеческого организма, а также порождает снижение бдительности из-за привыкания к факту появления ложных срабатываний.

Таким образом, при разработке проекта оборудования 00 техническими средствами охранной сигнализации помимо гаммы технических факторов необходимо учитывать факторы, определяемые поведением нарушителя.

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

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

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

С целью повышения устойчивости рубежей охраны к преодолению они должны оборудоваться СО, работающими на разных физических принципах действия, а также должна быть реализована функция дистанционного контроля. Комбинирование данных СО должно производиться по схеме М из N. Числа М и N определяются в ходе проектирования КТСО индивидуально для каждого рубежа охраны объекта.

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

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

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

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

I тип - с низкой устойчивостью к обходу;

II тип - со средней устойчивостью к обходу;

III тип - с высокой устойчивостью к обходу.

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

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

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

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

Для того чтобы оперативно обнаружить выход из строя составных частей КТСО, в том числе и в случае преднамеренных действий, применяется дистанционный контроль, обеспечивающий проверку работоспособности СО, соединительной линии и приемной аппаратуры ССОИ, а также повышающий устойчивость ТСОС к обходу соединительных линий и имитации работы СО.

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

Как показали результаты многих исследований, для выработки системного решения, удовлетворяющего необходимым и достаточным условиям обеспечения надежной защиты 00 от подготовленного и технически оснащенного нарушителя, требуется полный учет не только перечисленных выше факторов, но и многих других, как то: состояние инженерных сооружений объекта, состав и уровень подготовки сил физической охраны объекта, окружение объекта, характер объекта, расположение и количество сил поддержки, состояние сетей электропитания объекта и т.д.

Многолетний опыт по созданию систем защиты объектов убеждает в безусловной необходимости разрабатывать в каждом случае системную концепцию обеспечения безопасности конкретного объекта, которая на практике предполагает комплексное взаимоувязанное решение руководством предприятия и службой безопасности ряда крупных блоков задач, как то:

1. Определение стратегии комплексной безопасности.

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

2. Обеспечение безопасности от физического проникновения на территорию и в помещения объекта. В этом блоке задач на основе анализа доступности объекта моделируются стратегия и тактика поведения потенциального нарушителя; дифференцируются зоны безопасности; на основе определения ключевых жизненно важных центров объектов разрабатываются принципы и схемы оборудования техническими средствами охранной сигнализации и телевизионного наблюдения, средствами инженерной, технической и специальной защиты рубежей охраны. Соответственно, на основе расчета тактико-технических требований выбирается состав и номенклатура технических средств.

3. Защита информации. Решение задач данного блока обеспечивается специальными методами защиты. На основе разработки принципов проверки, классификации источников информации и каналов ее утечки разрабатываются концептуальные модели защиты от утечки информации, проводятся их оценки на предмет эффективности предлагаемых этими моделями решений. Здесь решается широкая гамма задач разработки методов защиты по всем возможным каналам утечки. Разрабатывается нормативная база по защите от утечки информации. На основе моделирования возможных способов приема информации потенциальным нарушителем за пределами помещений посредством применения направленных микрофонов, лазерных средств и т.п. вырабатываются методы пассивной и активной защиты.

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

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

6. Обеспечение безопасности в локальных вычислительных сетях и ПЭВМ, т.е. в автоматизированных системах обработки информации. Здесь на основе анализа моделей нарушителей, классификации видов угроз и видов компрометации информации разрабатывается комплексный подход к защите информации в автоматизированных информационных системах, ЛВС, серверах и ПЭВМ, соответствующая нормативно-правовая база защиты, регламентирующие документы; разрабатываются методы и способы программно-аппаратной защиты от несанкционированного доступа и копирования. Особое место занимают разработка и внедрение специальных математических и программных методов защиты операционных систем, баз данных и серверов, методов идентификации пользователей и ЭВМ, паролей, ключей и антивирусных программ. На основе определения и анализа задач СБ разрабатываются организационные меры защиты.

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

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

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

- разработка и реализация мероприятий по изучению лиц из числа персонала и иных лиц, в действиях которых содержатся угрозы безопасности деятельности учреждения посредством воздействия на его сотрудников, их близких и родственников;

- проверка кандидатов для приема на работу;

- разработка и реализация мероприятий по обеспечению "чистоты рук";

- организация взаимодействия и поддержание контактов с силами поддержки и/или правоохранительными органами по вопросам обеспечения безопасности и многое другое.

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

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

10. Организация системы контроля доступа. Этот блок задач направлен на эффективную реализацию процедур проверки человека, пытающегося открыто проникнуть на территорию объекта, в отдельные его помещения и режимные зоны. Здесь решаются задачи идентификации - это установление тождества по совокупности общих и частных признаков и аутентификации - это установление подлинности личности.

Кроме 10 перечисленных существуют иные блоки задач, рассматривающих как общесистемные проблемы, например, определение приоритетов во взаимодействии элементов системы безопасности, так и специальные, например обеспечение пожарной безопасности. Области охранной деятельности, связанные с реализацией названных задач, чрезвычайно многогранны. В данной работе рассматриваются лишь основы теории создания технических средств охраны, с помощью которых обеспечивается защита объекта охраны от физического проникновения нарушителя, т.е. решение второго блока задач.

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

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

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

В мировой практике уже давно используется такое понятие как система защиты, под которой подразумевается комплекс организационных и технических мероприятий, направленных на выявление и противодействие различным видам угроз деятельности объекта.

Рассмотрение возможных угроз проводится по следующим основным направлениям:

- безопасность персонала: неэффективная защита может привести к ущербу здоровью или даже угрозе жизни сотрудников;

- угрозы материальным ценностям, имуществу и оборудованию;

- безопасность информации.

Существенным при оценке угроз и выборе приоритетов в системе защиты является учет международного опыта по организации охранной деятельности применительно к объектам конкретного вида, например, банков, предприятий, крупных офисов и т.д. Этот опыт берется за основу и при подготовке современных нормативов защиты. Так, например, западноевропейские фирмы - производители оборудования для систем банковской защиты придерживаются единых критериев оценки угроз, согласно которым для сейфовых комнат - хранилищ ценностей и компьютерной информации приоритеты направлений защиты следующие:

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

- несанкционированный съем информации из компьютерного банка данных;

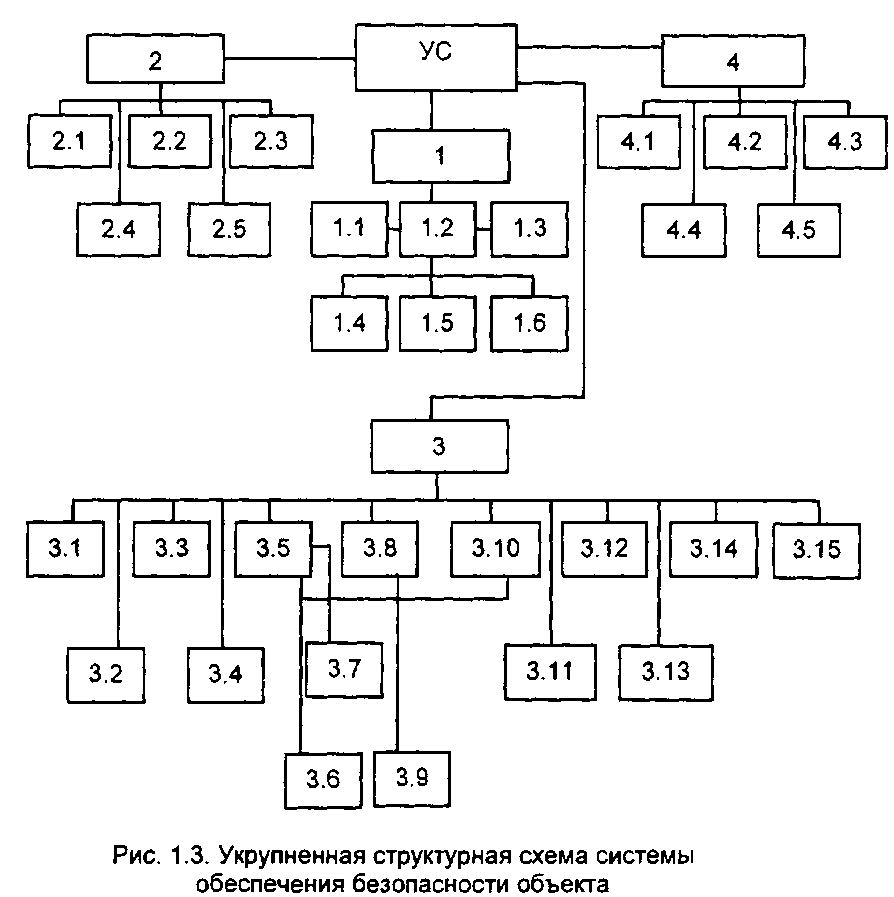
- несанкционированное проникновение в сейфовую комнату как с целью кражи ценностей, так и с целью кражи информации.

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

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

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

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



Таким образом, эффективность системы защиты оценивается величиной времени с момента возникновения угрозы до начала противодействия или ликвидации ее. Чем более сложная и разветвленная система защиты, тем больше времени потребуется на ее преодоление и тем больше вероятность того, что угроза будет своевременно обнаружена, определена и отражена.

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

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

На рис. 1.3 приняты следующие обозначения:

УС - укрупненная структурная схема системы обеспечения безопасности объекта

1 - физическая защита

1.1 - объектовая и/или городская пожарная команда

1.2 - служба охраны

1.3 - наряд милиции и/или силы поддержки

1.4 - работники контрольно-пропускного поста

1.5 - операторы технических средств охраны

1.6 - тревожная группа и подвижные посты

2 - инженерная защита

2.1 - усиленные ограждающие конструкции

2.2 - усиленные двери и дверные коробки

2.3 - металлические решетки и жалюзи

2.4 - спецзамки, усиленные запоры

2.5 - сейфы повышенной стойкости

3 - техническая защита

3.1 - средства обнаружения радиоактивных средств

3.2 - средства обнаружения оружия

3.3 - система пожарной сигнализации

3.4 - система тревожного оповещения

3.5 - система контроля доступа

3.6 - охранное освещение

3.7 - переговорные устройства

3.8 - система охранной сигнализации

3.9 - источник резервного электропитания

3.10 - система телевизионного наблюдения

3.11 - средства связи

3.12- средства проверки почтовой корреспонденции

3.13- средства обнаружения взрывчатых веществ

3.14- система защиты средств ВТ и ЛВС

3.15- средства обнаружения и защиты от технических средств проникновения через инженерные коммуникации, отверстия, проёмы и т.д.

4 - специальная защита

4.1 - обеспечение требований безопасности на этапе строительства

4.2 - проведение обследования помещений на наличие устройств съема информации

4.3 - спецпроверка технических средств передачи, обработки, накопления и хранения информации

4.4 - специальные защищенные помещения для переговоров

4.5 - средства спецзащиты сетей коммуникации

Физическая защита обеспечивается службой охраны, основной задачей которой является предупреждение несанкционированного физического проникновения на территорию, в здания и помещения объекта злоумышленников и их сдерживание в течение расчетного времени.

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

Техническая защита включает систему охранной сигнализации, систему телевизионного наблюдения, систему тревожного оповещения, автоматизированную систему контроля доступа, переговорные устройства, средства связи, пожарной сигнализации, средства проверки почтовой корреспонденции, охранного освещения, резервного электропитания, систему дежурного и тревожного освещения.

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

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

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

- обеспечение требований безопасности на этапах проектирования, строительства и эксплуатации зданий;

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

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

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

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

- осуществление специальных проверочных мероприятий по выявлению неблагонадежных сотрудников и лиц с психическими отклонениями.

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

Таким образом, мы рассмотрели основные положения обобщенной системной концепции обеспечения безопасности 00.

3. Общий подход к категорированию объектов охраны

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

Система охраны объекта, т.е. его периметра, территории, зданий, помещений - это сложный, многорубежный комплекс, включающий в себя физическую защиту, инженерные сооружения, технические средства охранной сигнализации, системы телевизионного наблюдения, системы контроля доступа и многое другое, что было рассмотрено в структурной схеме системы обеспечения безопасности объекта.

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

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

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

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

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

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

1 -я категория - особо важный объект;

2-я категория - особо режимный объект;

3- я категория - режимный объект;

4- я категория - нережимный объект.

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

В относительно самостоятельных территориальных образованиях могут создаваться свои перечни объектов, дополняющие общий, исходя из требований местных условий и возможностей самостоятельного финансирования расходов по их оснащению КТСО.

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

Априори следует полагать:

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

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

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

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

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

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

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

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

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