Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 6 (145)/2005

О проектировании систем безопасности современного технического уровня

СИСТЕМЫ БЕЗОПАСНОСТИ

ОТ РЕДАКЦИИ

По оценкам, содержащимся в различных источниках информации, общий объем рынка технических средств (ТС) безопасности в России на 2004 г. составил по порядку величины несколько сот миллионов долларов (эта оценка может быть заниженной). Из них:

- охранное телевидение — 22% (доля импортного оборудования до 80%);
- системы контроля и управления доступом (СКУД) — 18% (доля импортного оборудования составляет до 30%);
- ТС охраны периметра — 14% (доля импортного оборудования — до 50%);
- системы защиты от краж и пожарные сигнализации — 27% (доля импортного оборудования — до 60%);
- охранные сигнализации — 11% (доля импортного оборудования — до 20%).

Доля импортного телевизионного оборудования в структуре продаж возрастает, а среди средств сигнализации и охраны периметра — снижается. Доля интегрированных систем безопасности (ИСБ) в общем объеме продаж пока составляет несколько процентов, но характеризуется быстрым ростом. Затраты на проекты, связанные с внедрением ИСБ, в расчете на один объект, в несколько раз превышают расходы на отдельные ТС.

Объем договора на оснащение объекта ИСБ составляет от $40—$50 тыс. для небольшого офиса до нескольких миллионов долларов для элитного коттеджного поселка или территории крупного промышленного предприятия.

В целом, анализ данного сектора рынка обычно затруднен тем, что компании, работающие в нем, не стремятся раскрывать информацию о своих продажах. По усредненным данным производителей и поставщиков систем, спрос распределяется следующим образом. Основное количество потребителей находится в нефтегазовой (25%), энергетической (16%) отраслях и в силовых структурах государственного управления (22%). Самым быстрорастущим является сектор оборудования жилья (до 10%). Здесь определяющими факторами повышения спроса на системы безопасности стали повышение платежеспособности покупателей нового жилья и давление растущей преступности.

Большая часть потребителей ТС безопасности расположена в Центральном (37%), Уральском (23%) и Сибирском (12%) федеральных округах.

Рынок технических средств обеспечения безопасности растет довольно быстро. Каждый год объем оборотов на нем увеличивается от 10 до 35%, в зависимости от сектора. С учетом показателей роста по сегментам и объемов этих сегментов, Департамент консалтинга РБК в своем исследовании «Российский рынок систем безопасности» прогнозирует ежегодный рост рынка в 17—19%. Таким образом, в 2006 г. объем рынка средств безопасности превысит $1 млрд, а к 2008 г. достигнет $1,6 млрд.

Основными факторами развития рынка в упомянутом исследовании называются положительный финансовый климат в России, рост культуры использования систем безопасности, увеличение доли технических средств охраны российского производства, повышение рисков террористических угроз. Рост культуры потребителей систем безопасности выражается как в повышении уровня притязаний по качеству, так и в требовании к интегрируемости систем безопасности. С одной стороны, у пользователей накапливается некий объем установленных ранее систем и при внедрении новых систем требуется интеграция с уже имеющимися. С другой стороны, все больше клиентов осознают, что наиболее работоспособными являются именно интегрированные системы безопасности.

В последнее время соответствующим руководителям или собственникам объектов все серьезнее приходится задумываться о сохранности имущества предприятий, корпораций или просто домовладений. Рано или поздно выясняется, что для организации охраны того или иного имущества и построения надежной ИСБ необходимо подобрать технические средства, значит, нужна самая последняя и полная информация в области современных технологий, а ее, как правило, не хватает. Специалисты из собственной охранной службы предприятия, эксплуатирующие существующие системы, также в большинстве случаев оказываются не в курсе передовых достижений в области технического обеспечения безопасности.

Чтобы решить задачу оснащения предприятия системой безопасности эффективно и без лишних затрат, целесообразно поручить разработку ИСБ сторонним специалистам. Услуги по разработке ИСБ современного технического уровня достаточно широко представлены на рынке продуктов безопасности, и заказчик может выбрать наиболее оптимальный для себя вариант.

В данной публикации содержится информация, которая поможет разобраться в свойствах решений, предлагаемых различными специалистами в области построения ИСБ.

Дмитрий Огородников,
начальник отдела проектирования защищенных сиситем
e-mail: berd@jet.msk.su

О проектировании систем безопасности современного технического уровня

Дмитрий Беседин,
главный специалист по интегрированным системам безопасности

СОДЕРЖАНИЕ

Введение

Мир, в котором мы живем, небезопасен. Причем похоже, что с течением времени ситуация ухудшается. Современному человеку достаточно часто приходится сталкиваться с проблемой защиты своих интересов от различных посягательств.

Во все времена основная цель большинства злоумышленников была одной и той же — завладеть чужим имуществом и извлечь из этого выгоду. В данном случае термин «имущество» употребляется в самом широком смысле. Это могут быть участки земли, здания, любое оборудование, транспортные средства, культурные ценности и многое другое. История изобретения человеком способов защиты своей собственности не менее длинна, чем вся история цивилизации. Практически все технологические достижения, которые можно использовать для охраны чего бы то ни было, сразу использовались при решении данных задач.

В последнее время охранные системы достигли столь высокой степени развития, что для управления ими необходимо применение специализированных компьютеров. На техническом языке такие системы называются интегрированными системами безопасности (ИСБ). С одной стороны, это, конечно, достижение, и такая система имеет лучшие технические характеристики, эффективнее и удобнее в работе, чем примитивная сигнализация, собранная из проволочки, реле и звонка. Однако за высокую эффективность ИСБ приходится платить ее сложностью. ИСБ требуют не только профессиональной разработки и установки, но и хорошей технической подготовки сотрудников службы охраны объекта, на котором она устанавливается. К тому же оборудование объекта средствами ИСБ требует существенных денежных затрат.

Возникает вопрос — почему необходимо непрерывное техническое совершенствование систем безопасности и в чем причина резкого ускорения этого процесса в последнее время? До наступления научно-технической революции все было

иначе... На протяжении многих предыдущих веков наши предки решали задачу охраны просто — строили заборы и заводили собак.

Кстати, о собаках. Несколько неожиданным, на первый взгляд, будет утверждение, что сторожевая собака может служить примером хорошей ИСБ. Однако данная «система безопасности» и в самом деле имеет почти все необходимые для построения ИСБ элементы:

- сенсоры (датчики обстановки) — глаза, уши, нос и прочие органы чувств;
- приемно-контрольное «устройство» — нервная система;
- «программное управление» — навыки, привитые дрессировкой;
- система опознавания «свой — чужой»: собака узнает хозяев;
- устройство подачи сигнала тревоги — способна лаять...

Кроме того, собака обладает качествами, которых пока еще нет у большинства современных ИСБ:

- автономной подвижностью по охраняемой территории;
- некоторой свободой в принятии самостоятельных решений;
- способностью самостоятельно противодействовать нарушителям;
- также можно смело утверждать, что данная «система» проверена в эксплуатации на протяжении нескольких тысяч лет и достаточно экономична в обслуживании.

Все перечисленные достоинства компактно размещены и интегрированы между собой в довольно симпатичном существе.

Несмотря на все эти достоинства, следует признать, что охрана объектов с помощью собак постепенно становится все большей редкостью, уходя в прошлое, поскольку данная «система обеспечения безопасности» имеет и серьезные недостатки:

- охранная функция собаки локальна — работает только в том месте, где она непосредственно находится;
- «интерфейс» передачи информации к оператору специфичен по исполнению и весьма индивидуален — чтобы понять, о чем собака хочет сообщить своим поведением, человеку надо хорошо знать именно эту собаку;
- командное управление также локально и построено на базе нечеткой логики — передача команд возможна только рядом с человеком, а исполнение не гарантировано и зависит от внешних обстоятельств;
- возможности интеграции с другими системами практически отсутствуют.

При ближайшем рассмотрении любой не интегрированной локальной системы безопасности (ЛСБ) становится очевидным, что они страдают теми же «собачьими» недостатками. Практически все недостатки локальных технических систем безопасности относятся к группе коммуникационных характеристик.

Итак, общую тенденцию технологического развития систем безопасности на современном этапе можно сформулировать следующим образом: **локальные системы, не имеющие развитых возможностей обмена информацией со своим окружением (оператором, объектом, другими системами и т.д.), необратимо устаревают и выходят из практического употребления**. На смену ЛСБ приходит новое техническое поколение систем — ИСБ, построенные на современной технологической базе.

Как уже отмечалось выше, ИСБ является сложной системой технических средств, требующей профессионального подхода при разработке, установке на объекте и эксплуатации. Но выбор конкретного варианта реализации ИСБ остается функцией заказчика. Далее будет показано, на что в первую очередь следует обратить внимание при выборе эффективного, по соотношению затрат и качества, варианта объектовой ИСБ. Будут рассмотрены следующие основные вопросы:

- обследование объекта защиты — на что необходимо обращать внимание при обеспечении безопасности различных объектов;
- угрозы объекту: откуда и какой опасности следует ожидать;
- требования к решению по защите объекта и схема решения;
- применяемые технические средства;
- управление создаваемой системой и ее техническая эксплуатация;
- организационные вопросы создания и развертывания ИСБ.

В практической работе ответы на данные вопросы образуют основу общей концепции безопасности объекта, защищаемого при помощи ИСБ. Анализ общей концепции безопасности весьма полезен, так как позволяет оценить эффект от внедрения ИСБ и достаточно точно для целей краткосрочного планирования (на 1—3 года) подсчитать затраты на ее развертывание.

Обследование объекта

Рассмотрим процедуру обследования объекта, имеющего собственную территорию, капитальные сооружения (здания), инженерную инфраструктуру (магистрали электро-, водо-, теплоснабжения и прочее), транспорт, а также обслуживающий персонал. Небольшой частный дом или офис обследуется по тем же правилам, но часть шагов при этом можно будет исключить.

Целью данного этапа является получение актуальной и достоверной информации о текущем состоянии безопасности объекта. Состав работ включает сбор следующих сведений о самом объекте и об установленных на нем технических средствах безопасности.

1. Расположение объекта, окружающей местности и застройки (желательно получение или составление топографической схемы или плана местности с указанием размещения объекта). В случае, если объект занимает одно или несколько помещений в многоэтажном здании, требуется поэтажный план с указанием помещений, занимаемых объектом и смежных с ним.
2. Сведения об имевших место несанкционированных проникновениях на объект, включая попытки; прочие сведения о попытках атак на объект с указанием последствий, а также случаев и происшествий, ранее нарушавших безопасность объекта.
3. Характеристика ограждений и стен объекта, наличие проходов и проездов, дверей, ворот и прочих управляемых и неуправляемых преграждающих устройств. Наличие и расположение окон и прочих проемов, крыш, подвалов и чердаков.
4. Сведения о количестве и времени прохода лиц, которым разрешен доступ на объект.
5. Сведения об установленных на объекте средствах контроля и управления доступом (проходом на объект) о наличии централизованного управления указанными средствами, режимах и расписании работы.
6. Технические сведения об установленных на объекте средствах сигнализации, позиции датчиков, схемы подключения, режимы работы, расположение постов дежурных операторов.
7. Наличие средств массового оповещения и сигнализации о нарушениях режима безопасности объекта.
8. Информация об имеющихся на объекте средствах наблюдения: места установки камер, зоны обзора, наличие тревожной автоматики, устройств записи, мониторов, наблюдаемых операторами, и т.д.
9. Наличие пункта (поста) централизованного наблюдения, средств интеграции отдельных ТС в систему, автоматического управления интегрированной системой и дежурства операторов.
10. Наличие вспомогательных технических средств, обеспечивающих функционирование ТСБ.

Результатом этапа обследования обычно является характеристика (описание) объекта защиты — структурированная детальная информация, необходимая для проведения оценки состояния безопасности, разработки актуальной модели угроз для объекта, эскиза эталонного решения по защите объекта и рекомендаций по изменению или дополнению действующей политики безопасности и частных решений по защите объекта.

Специалисты, проводящие обследование, обязательно должны выехать на объект. Не следует особенно доверять предложениям организаций, обещающих разработать схему обеспечения безопасности объекта только на основании документов — скорее всего вам будет предложена типовая схема и комплектация того, что эта компания хочет продать. К реальным нуждам безопасности конкретного объекта эти предложения могут иметь весьма отдаленное отношение...

Если на объекте на момент обследования вообще не установлены ТС безопасности (обычно это бывает на вновь сооружаемых объектах), все вышеперечисленные пункты должны рассматриваться с позиции: «а где эти технические средства полезно и возможно установить?»

Анализ текущего уровня защищенности объекта

Для построения надежной ИСБ необходима предварительная оценка текущих показателей защищенности объекта. При решении этой задачи проводится анализ следующих данных:

1) местоположение и окружение объекта;
2) действия и проявления выявленных угрожающих факторов;
3) соответствие положений действующей политики безопасности указаниям, содержащимся в руководящих документах вышестоящих организаций, и реально сложившейся на объекте и вокруг него обстановке;
4) правильность выбора, размещения и настройки технических средств безопасности с точки зрения реализации действующей политики безопасности и режимных мероприятий;
5) опыт реагирования имеющихся ТСБ объекта на предыдущие нарушения режима безопасно-

сти и происшествия, включая зарегистрированные попытки нарушений;
6) информация об эксплуатационной надежности установленных ТСБ, выявленных отказах и сбоях;
7) результаты предыдущих проверок защищенности объекта.

Результатом работ на этапе анализа защищенности является оценка эффективности используемых средств и методов защиты объекта. Для более полного анализа текущего уровня защищенности дополнительно проводится анализ текущей политики безопасности объекта с построением модели угроз, а также инструментальный анализ защищенности объекта с помощью общих и специализированных технических средств.

Анализ текущей политики безопасности

В процессе выполнения работ проводится проверка наличия у заказчика нормативно-регламентирующей базы по обеспечению безопасности проверяемых объектов, в которую входят:
1) инструктивно-регламентирующая документация с установлением обязанностей по обеспечению безопасности объекта для сотрудников всех должностей;
2) утвержденная политика обеспечения безопасности объектов;
3) документированное обоснование выбора применяемых средств и мер защиты обследуемого объекта;
4) раздел в правилах внутреннего распорядка, регламентирующий соблюдение сотрудниками режима безопасности, установленного на объекте;
5) регламент эксплуатации и инструкции операторам установленных ТСБ.

Результатом анализа политики безопасности является документ, содержащий оценку полноты выполнения действующих нормативно-регламентирующих документов, а также эффективности существующей политики и режима обеспечения безопасности.

С учетом результатов анализа эффективности существующих политики и режима безопасности объекта в дальнейшем составляются рекомендации по разработке (или доработке) политики обеспечения безопасности и режимных мероприятий объекта.

Большое влияние на формирование выводов при обследовании объекта оказывает его вид и функциональное назначение. Выводы не обязаны быть строго формализованными, но должны давать представление об основных свойствах объекта. Например, резюме результатов обследования может выглядеть следующим образом:

Защищаемый объект представляет собой вновь сооружаемый коттеджный поселок. Тип застройки — малоэтажные дома, построенные по индивидуальным проектам. Стоимость строений и внутреннего оборудования высокая. Дома расположены на отдельных участках, как правило, в середине участка. Электро-, водо-, газоснабжение, канализация — централизованные. Имеется отдельная канализация для слаботочной сети сигнализации и связи. Отопление производится от газовых котлов в каждом доме.

Поселок расположен в равнинной местности с небольшим перепадом высот, его территория пересечена ложбиной с протоком воды. Граница территории поселка представляет собой неправильный многоугольник с большим числом углов на внешнем периметре. Часть территории поселка занята высокоствольным смешанным лесом с преобладанием сосны. Подлесок густой, засоренный валежником. Грунт — суглинок. Подпочвенные воды — близко к поверхности.

Существующая ограда представляет собой декоративную металлическую решетку высотой около 2,5 м, закрепленную на кирпичных (по фасаду) или металлических полых столбах. Ограда выстроена по границе землеотвода. Вплотную к ограде изнутри примыкают участки, которые выкуплены в частную собственность. Инженерное оборудование ограды и проводка вдоль нее отсутствуют. На фасадной части, примыкающей к основному въезду, ограда оборудована освещением. На некоторых участках периметра, проходящих по лесу, ограждение отсутствует. Конструкция ограды такова, что ее легко преодолеть (перелезть).

Дома поселка вместе с участками реализуются в собственность лицам с высоким уровнем доходов для круглогодичной эксплуатации. Для эксплуатации поселка планируется организация управляющей компании (УК).

Наиболее вероятно, что большинство домов будет использоваться для круглогодичного проживания или отдыха по выходным семьями с детьми. Часть домов будет эксплуатироваться как холостяцкие или дома приемов. Количество жителей, находящихся на территории поселка, будет заметно изменяться в зависимости от сезона и дня недели. Соответственно, будет меняться интенсивность перемещения людей по территории и нагрузка на инженерную инфраструктуру.

В непосредственной близости от основного въезда в поселок будет построен торгово-развлекательный комплекс со свободным доступом извне территории поселка. Управление эксплуатацией

данного комплекса будет осуществляться той же УК, что и поселка.

В качестве примера в даном случае мы преднамеренно рассмотрели объект непроизводственного характера, но с высокими требованиями к режиму, чтобы показать универсальность применяемой методики обследования.

К результатам обследования полезно приложить план объекта, нанесенный на топографическую схему прилегающей территории. Масштаб схемы следует выбирать по возможности более крупным, чтобы на ней можно было отобразить прокладку инженерных магистралей. Лучше всего иметь копию схемы на компьютерном диске в одном из распространенных форматов. На одной из копий схемы следует впоследствии нанести расположение технических средств безопасности и соединяющие их кабельные линии.

Построение модели угроз и модели нарушителя

Термины «модель угроз» и «модель нарушителя» являются стандартными для профессиональной и околопрофессиональной литературы по безопасности. Не вникая в их точное определение, рассмотрим практическое приложение данных понятий к разработке комплекса мер по обеспечению безопасности реального объекта.

Прежде всего, необходимо понять, что угрозы существуют постоянно. Среди окружающих людей всегда найдутся такие, кто рассматривает ваше имущество как свою законную добычу, а некоторые из них даже готовы подавить ваше сопротивление, если вы не захотите его отдать. Уровень опасности, исходящей от потенциальных и действующих правонарушителей, никак не зависит от ваших усилий по обеспечению безопасности. Уровень преступности, характерный для места расположения вашего объекта, является результатом общественных отношений, сложившихся в данном районе. Поэтому и воспринимать криминальную угрозу следует как объективную реальность — на вас нападут. Обязательно. И только от вашей подготовленности зависит, к каким результатам приведет это нападение.

Есть еще ряд постоянно существующих опасностей. Они связаны с ограниченной надежностью технических средств, которыми оборудован объект. Прежде всего, это пожары. Любое устройство, питающееся электроэнергией или использующее топливо, может при неправильном функционировании самовозгореться. Также следует учитывать возможности аварии трубопроводов газа, воды (в том числе теплоцентрали — горячая вода под высоким давлением может нанести ущерб не меньший, чем огонь) и конструкций здания (редко, но бывает).

Следующая группа угроз — это технические неисправности. Отказ любого элемента инженерной инфраструктуры может привести к частичному или полному прекращению работы объекта в целом. Кроме того, неправильная работа или отказ одних устройств может вызвать повреждение других. Например, если в зимних условиях отключается электропитание насосов, перекачивающих воду в системе отопления, то через некоторое время вода, застоявшаяся в трубах, охладится до точки замерзания и разорвет их.

Нельзя исключать из числа угроз и несчастные случаи, как специфически связанные с работой на объекте, так и общего характера, а также возможность проявления приступов заболеваний и последствий неправильного образа жизни.

Все объекты подвержены влиянию стихийных сил. Для любого места расположения объекта обычно доступны усредненные данные о погодных условиях и максимальных значениях скорости ветра, уровня паводка и т.п. Учет природных факторов должен проводиться двояко: как угроз объекту защиты в целом и как условий, даже в случае крайних значений которых должно быть обеспечено функционирование ИСБ объекта.

Отдельно следует рассмотреть угрозы информационной безопасности. Обычно этот термин применяется к информационным системам (ИС) предприятий и объектам, оборудованным такими системами. Корпоративные ИС снабжаются подсистемой информационной безопасности (ПИБ), для построения которой выполняется отдельная серьезная разработка. Не рассматривая подробно построение ПИБ, отметим следующее:

- современные ПИБ стыкуются с ИСБ и обмениваются с ней информацией;
- центральная часть ИСБ строится на базе средств вычислительной техники и может рассматриваться как особо выделенный сегмент ИС предприятия;
- средства ИСБ и находящаяся в них информация о защищаемом объекте нуждаются в защите собственным сегментом ПИБ.

Кроме угроз ИС и компьютерной части ИСБ, возможны и другие угрозы информационной безопасности объекта. К ним относятся утечки и преднамеренный сбор информации:

Рис. 1 Цели разработки модели угроз

- об объекте и предприятии, к которому он принадлежит;
- о лицах, работающих или присутствующих на объекте;
- о хранимых ценностях и имуществе;
- о прочих предметах, являющихся потенциальными целями преступного посягательства.

В качестве примера представим общую описательную модель угроз, составленную для разработки концепции безопасности жилого комплекса типа таун-хаус в ближайшем Подмосковье.

Основными факторами, обуславливающими формирование угроз, являются:

- расположение объекта в ближнем Подмосковье — зоне активного действия преступных групп;
- высокая стоимость имущества, находящегося на территории объекта;
- высокий уровень дохода жителей.

На комплекс и проживающих в нем лиц воздействуют следующие виды угроз.

Криминальные угрозы

Преднамеренные нападения: причинение телесных повреждений, разбои, грабежи, хищения, угоны транспорта, вандализм, хулиганство.

Проявления организованной преступности: основными видами ожидаемых проявлений организованной преступности на территории комплекса являются вымогательство и сбыт наркотиков[1].

Проникновение наркоторговцев будет иметь целью организацию сбыта наркотических веществ в основном среди молодежи, составляющей значительную часть проживающих и гостей комплекса.

Прочие виды правонарушений: работа торгово-развлекательного центра (большого магазина) на территории комплекса обязательно привлечет к нему внимание правонарушителей со следующими криминальными специализациями: хищения из машин, карманные кражи, хищения в торговом зале. Материальный ущерб, причиняемый этими видами правонарушений, невелик, но эти правонарушения способны нанести значительный ущерб репутации администрации торгового центра.

Терроризм: Отдельно следует отметить угрозу терроризма. Как показывает практика, отразить и нейтрализовать неожиданно нападающую организованную и хорошо вооруженную группу преступников крайне сложно, в то же время проведение террористического акта на защищаемом объекте маловероятно. Поэтому наиболее целесообразно подготовить службу безопасности не столько к предотвращению террористической атаки, сколько к минимизации ее последствий. Это потребует мини-

1 Следует отметить, что основным объектом вымогательства может стать компания, управляющая комплексом. Способом вымогательства — угроза организации саботажа (т.е. преднамеренного отключения или повреждения электропитания, водоснабжения и прочих элементов инженерной инфраструктуры). Высокая стоимость оборудования и сооружений комплекса повышают опасность причинения крупного ущерба в результате саботажа.

мальных финансовых затрат и будет сводиться к разработке соответствующих инструкций для сотрудников службы безопасности.

Прочие угрозы здоровью и жизни

Случаи медицинского характера: несчастные случаи, острые заболевания, травмы, ранения.

Случаи условно-медицинского характера: последствия злоупотребления алкоголем, медицинскими и наркотическими препаратами.

Угрозы этой группы могут потребовать экстренной реакции непосредственно после реализации угрозы, т.к. пострадавший может находиться в тяжелом состоянии, угрожающем его жизни.

Утечки информации о частной жизни

Серьезную угрозу для многих проживающих может представлять утечка информации об их частной жизни. Возможно проникновение на территорию жилого комплекса посторонних лиц с задачей сбора компрометирующей информации. Такими лицами могут быть сотрудники частных детективных агентств, работающие против кого-либо по найму, журналисты и т.п.

Другим каналом утечки информации могут стать сами сотрудники службы безопасности. При выполнении служебной задачи по защите объекта у охраны накапливается и хранится информация о времени приезда и отъезда посетителей, составе приглашенных гостей, номерах машин и многое другое.

Технические угрозы

Загорания: случайные, от неисправностей технических систем, преднамеренные поджоги.

Выход из строя технических систем инженерной инфраструктуры (электро-, водо , газоснабжение, канализация). Причинами могут быть: случайные отказы, неверные действия обслуживающего персонала, преднамеренные действия. Реализация данной угрозы может причинить существенный материальный ущерб в результате поломки оборудования. Кроме того, возможны нарушения работы взаимодействующих систем.

Аварии на сетях электроснабжения. Ввиду важности бесперебойного электроснабжения для работы всех инженерных систем, включая технические средства системы безопасности, данная угроза выделена в отдельную группу. Электроснабжение объекта осуществляется с одной точки подключения. В случае пропадания питания на точке подключения в результате аварии или преднамеренного отключения, электроснабжение будет полностью прервано.

Стихийные угрозы

В эту категорию входят: затопления цокольных частей зданий, объектов инженерной инфраструктуры, кабельной канализации; угроза затопления кабельной канализации; повреждения от ветровых нагрузок и т.д.

Для наглядности *модели угроз* полезно свести данные в таблицу (см. табл. 1). Здесь же можно предварительно планировать меры, силы и средства для отражения выявленных угроз. Как правило, планирование осуществляется, исходя из возможностей службы безопасности (СБ), постоянно обслуживающей или формируемой для защиты рассматриваемого объекта.

При обследовании объекта специалистами модель угроз строится с помощью специального вопросника, который содержит названия предполагаемых угроз, сгруппированные по категориям, и некоторые количественные параметры для оценки их силы (опасности) и вероятности проявления. Для объектов, по которым не требуется проводить аттестацию на соответствие требованиям какого-либо нормативно-технического документа, модель угроз может быть составлена в форме текстового описания.

Модель нарушителя тесно связана с моделью угроз и обычно является ее частью. Смысловые отношения между ними следующие. В модели угроз содержится максимально полное описание опасностей для объекта. В модели нарушителя конкретизируется: кто, какими средствами и с использованием каких знаний может реализовать угрозы и нанести ущерб объекту.

При оценке соотношения между моделями угроз и нарушителя важно понимать, что' на самом деле является целью атаки нарушителя и объектом защиты. Например, если целью атаки на ваш частный дом является попытка помешать вашему бизнесу, то эта угроза должна учитываться в модели угроз предприятия (бизнеса). Нарушитель, которого в данном случае следует ожидать, окажется намного более сильным и квалифицированным, чем можно было бы предположить из модели угроз, составленной для объекта «дом».

После того как специалисты, проведя необходимые исследования, составили и предложили заказчику описание объекта и полную модель угроз, следует разработать решение по защите объекта.

Табл. 1 Модели угроз

Угрозы	Объект посягательства	Способы борьбы	Подразделение СБ	Технические средства	Последствия
Криминальные угрозы					
Разбой, причинение телесных повреждений	Здоровье и имущество жителей	• Оперативная работа по предупреждению • Реакция патрульной службы	• Оперативная группа • Дежурная служба • Патрульная служба	• Средства связи • Вооружение • Сигнализация в домах • Патрульный транспорт	Тяжелые последствия, крупные убытки
Грабежи, кражи	Имущество	• Оперативная работа по предупреждению • Реакция патрульной службы • Охрана домов	• Оперативная группа • Группа общественной безопасности • Дежурная служба • Патрульная служба • Техническая группа	• Сигнализация в домах • Сигнализация на периметре • Патрульный транспорт • Средства связи	Убытки, последствия средней тяжести
Угоны автотранспорта	Автомобили на территории	• Оперативная работа по предупреждению • Режим проезда через КПП • Реакция патрульной службы	• Оперативная группа • Дежурная служба • Патрульная служба	• Средства связи • Преграждающие устройства КПП • Система телевизионного наблюдения	Заметные убытки
Вандализм, хулиганство	Имущество, личное достоинство и здоровье	• Оперативная работа по предупреждению • Реакция патрульной службы • Охрана домов • Работа по взысканию ущерба	• Группа общественной безопасности • Дежурная служба • Патрульная служба • Техническая группа	• Система телевизионного наблюдения • Сигнализация в домах • Сигнализация на периметре	Убытки, ущерб репутации
Криминальные угрозы от организованной преступности					
Терроризм	Жизнь людей на объекте и финансовые средства	• Оперативная работа по предупреждению • Реакция патрульной службы, блокирование КПП • Оповещение жителей • Взаимодействие с правоохранительными органами	• Руководство СБ • Дежурная служба • Оперативная группа • Патрульная служба • Дежурные по КПП	• Преграждающие устройства КПП • Сигнализация на периметре • Система телевизионного наблюдения	Потери в людях, крупные убытки
Вымогательство	Финансовые средства управляющей компании	• Оперативное противодействие • Взаимодействие с правоохранительными органами	• Руководство СБ • Оперативная группа	• Средства скрытой видео- и звукозаписи	Вплоть до потери бизнеса
Сбыт наркотических веществ	Жизнь и здоровье	• Оперативное противодействие • Взаимодействие с правоохранительными органами • Психологическая помощь жителям	• Оперативная группа • Группа общественной безопасности • Патрульная служба	• Средства скрытой видео- и звукозаписи	Тяжелые, крупные убытки
Прочие криминальные угрозы					
Нарушения пропускного режима	Общая безопасность	• Работа службы КПП • Реакция патрульной службы	• Дежурная служба • Патрульная служба • Дежурные по КПП	• Сигнализация на периметре • Система телевизионного наблюдения	Подготовка других посягательств

Табл. 1 Модели угроз (окончание)

Угрозы	Объект посягательства	Способы борьбы	Подразделение СБ	Технические средства	Последствия
Угрозы здоровью					
Заболевания, отравления	Жизнь и здоровье	• Работа дежурной службы • Работа медицинской группы	• Дежурная служба • Медицинская группа	• Средства связи • Сигнализация в домах	До очень тяжелых
Травмы, ранения	Жизнь и здоровье	• Работа дежурной службы. • Работа медицинской группы	• Дежурная служба • Медицинская группа	• Средства связи • Сигнализация в домах	До очень тяжелых
Злоупотребление алкоголем и пр.	Жизнь и здоровье	• Реакция патрульной службы • Работа медицинской группы	• Дежурная служба • Группа общественной безопасности • Медицинская группа	• Средства связи • Система телевизионного наблюдения	До очень тяжелых
Утечки информации о частной жизни					
Утечки персональной информации	Репутация, финансовые средства	• Работа дежурной службы • Реакция патрульной службы • Оперативная работа	• Группа общественной безопасности • Дежурная служба • Патрульная служба • Дежурные по КПП	•Сигнализация на периметре • Система телевизионного наблюдения • Средства скрытой видео- и звукозаписи	Ущерб репутации, крупные убытки
Технические угрозы					
Пожары	Имущество, жизнь, здоровье	• Работа дежурной службы • Действия нештатного пожарного расчета	• Дежурная служба • Патрульная служба • Нештатный пожарный расчет • Техническая группа	• Сигнализация в домах •Пожарная техника • Система телевизионного наблюдения	Крупный ущерб, тяжелые последствия
Аварии инженерной инфраструктуры	Имущество, здоровье	• Работа дежурной службы • Взаимодействие со службами эксплуатации	• Дежурная служба	• Сигнализация на объектах инфраструктуры • Система телевизионного наблюдения	Крупный ущерб
Стихийные угрозы					
Затопления	Имущество	• Взаимодействие со службами эксплуатации	• Дежурная служба • Техническая группа		Крупный ущерб
Повреждения от ветровых нагрузок	Имущество, жизнь, здоровье	• Работа дежурной службы • Взаимодействие со службами эксплуатации	• Дежурная служба • Техническая группа	• Система телевизионного наблюдения	Ущерб, тяжелые последствия

Решение по защите объекта

Требования к решению по защите объекта

Требования к решению по защите объекта выдвигаются в результате сопоставления основных свойств защищаемого объекта с составленной на предыдущем этапе моделью угроз. Основные требования обычно схожи даже для существенно различающихся объектов. Наиболее общие из них приведены ниже.

Решение по защите (РЗ) должно учитывать уже принятые и реализованные в строительстве объекта проектные решения.

РЗ должно быть комплексным, это диктуется необходимостью противодействия совокупности одновременно действующих угроз. РЗ должно учитывать тот факт, что многие угрозы имеют активный характер, т.е. являются результатом преднамеренных действий, направленных на причинение вреда объекту.

Решение по защите должно соответствовать территориальной структуре объекта, т.е. учитывать реально складывающееся разделение объекта на зоны с разноплановыми постройками и различными возможностями и требованиями по обеспечению режима безопасности.

РЗ должно быть гибким в плане соответствия календарному и суточному графику работы объекта.

Отдельную группу требований к РЗ составляют требования по его выполнимости. Выдвигая требования или включая какие-либо пункты в РЗ, надо заранее представлять, кем и как они будут выполняться.

РЗ для крупного объекта, отвечающее вышеперечисленным условиям, очень трудно успешно реализовать при помощи одного или нескольких отдельных технических средств безопасности. Также невозможно обеспечить его исполнение только действиями охраны. В современных условиях для реализации РЗ создаваемая или существующая **служба безопасности** объекта должна быть оснащена комплексом **интегрированных** технических **средств безопасности – ИСБ**. В данном случае только комплексный подход позволяет добиться выполнения РЗ с необходимым уровнем надежности и качества.

Расчет установки технических средств необходимо проводить, исходя из возможностей и количественного состава службы безопасности. Примерный расчет сил территориальной СБ приведен ниже. Он производился для задачи обеспечения безопасности отдельно расположенного жилого массива (поселка), не имеющего на своей территории отдела внутренних дел, с площадью застройки, составляющей несколько квадратных километров.

Административная структура службы безопасности

Наиболее целесообразно сформировать СБ в виде отдельного частного охранного предприятия (ЧОП), которое принадлежит компании, осуществляющей эксплуатацию жилого массива. Между собственником объекта и ЧОП заключается договор об охране. Таким способом обеспечивается необходимая самостоятельность руководства ЧОП в принятии решений, находящихся в их компетенции, и, с другой стороны, полная зависимость ЧОП от собственника объекта, как единственного учредителя и заказчика.

Кадровая структура службы безопасности

Наиболее целесообразно построить ЧОП со следующей структурой.

Директор ЧОП, он же – начальник СБ.

Два заместителя: 1-й – по основному профилю, 2-й – по техническим средствам, оборудованию и обучению личного состава.

Оперативная группа (ОГ) в составе двух человек при ненормированном рабочем дне. Основная задача оперативной группы – сбор и анализ информации о готовящихся правонарушениях, направленных на причинение ущерба объекту. В задачу оперативной группы также входит предотвращение или минимизация вреда, причиняемого действиями организованных преступных групп. Сотрудники ОГ занимаются непосредственным выявлением лиц, совершающих или готовящих правонарушения на территории поселка, осуществляют их розыск, задержание и передачу правоохранительным органам.

Группа общественной безопасности (ОБГ) в составе двух человек при ненормированном рабочем дне. Основная задача этой группы – взаимодействие с лицами, проживающими на территории, с целью сбора информации о факторах, которые могут привести или уже привели к ущербу и нарушению безопасности объекта. Сотрудники группы должны оказывать жителям действенную организационную, психологическую и консультационную помощь, направленную на укрепление безопасности проживания. Сотрудники ОБГ должны вести прием граждан, обращающихся в СБ по вопросам охраны, режима и безопасности проживания, установки в частных владениях дополнительного оборудования безопасности, систем наблюдения, сигнализации и т.п.

Техническая группа (ТГ) в составе двух человек для проведения эксплуатационного обслуживания установленных технических средств безопасности. В задачу группы также входит: монтаж и подключение абонентских комплексов сигнализации в домах по заказу проживающих, устранение неисправностей всех технических средств безопасности поселка и взаимодействие с организацией, осуществляющей их техническое сопровождение. Сотрудники ТГ должны следить за исправностью и технической готовностью средств сигнализации на периметре территории, бесперебойностью работы средств телевизионного наблюдения, реагировать на заявки о неисправностях технических средств безопасности, установленных на территории и в частных домах поселка.

Дежурная служба в составе 8 человек (четыре смены по два человека). Осуществляет дежурство на **пульте централизованного наблюдения (ПЦН)** на всех технических средствах безопасности, установленных на территории поселка, и командование постами и патрульными. Наиболее целесообразный режим работы – сменный.

Постовая служба в составе, соответствующем количеству КПП и режиму их работы для несения службы на КПП.

Патрульная служба в составе 12 человек (четыре смены по 2 + 1). Предназначена для реагирования на сообщения о нарушениях периметра, срабатывания сигнализации и оказания помощи при напа-

дениях на проживающих на территории поселка. В случае необходимости патрульные должны помогать оперативной группе при проведении задержаний правонарушителей. Третий человек в составе дежурной смены патрульной службы нужен для повышения надежности реагирования на нарушения, происходящие одновременно в разных местах территории поселка.

Медицинская служба в составе трех человек при ненормированном рабочем дне с возможностью экстренного вызова. Основная задача — оказание экстренной медицинской помощи в случаях по профилю СБ или обращениях проживающих в отсутствие других возможностей получения помощи.

Итого, 48 человек личного состава, с учетом подмены при отпусках — 52 человека. В соответствии с назначением и функциями защищаемого объекта, состав СБ может изменяться как численно, так и по назначению групп. Например, для нежилых объектов не нужна группа общественной безопасности и в некоторых случаях не нужна оперативная группа. Для охраны предприятия, в состав которого входят склады и грузовой терминал, требуется более многочисленная патрульно-постовая служба.

Технические средства

Конфигурация технических средств безопасности определяется назначением ИСБ. Рассмотрим достаточно полную типовую конфигурацию. Устанавливаемая на объекте **совокупность технических средств безопасности (ТСБ)** должна выполнять следующие группы функций:

- регулирование перемещения людей и подвижных объектов по контролируемой территории и доступа в здания и отдельные помещения;
- обнаружение нарушений установленного на территории регламента перемещения людей и подвижных объектов;
- наблюдение за территорией объекта с записью результатов;
- сбор данных от устройств обнаружения и их централизованная обработка;
- выполнение заранее определенной совокупности действий по заданным сигналам;
- распознавание людей и подвижных объектов, пытающихся проникнуть и несанкционированно проникших на территорию и в сооружения (помещения) объекта;
- оповещение сотрудников службы безопасности и находящихся на объекте людей о нештатных ситуациях (тревогах).

Для выполнения перечисленных групп функций необходимо иметь:

- сенсоры (датчики обстановки);
- приемно-контрольные приборы;
- программное управление;
- систему опознавания «свой — чужой»;
- устройство подачи сигнала тревоги.

При «классическом» подходе к оборудованию объекта на нем устанавливаются несколько систем ТСБ, каждая из которых решает отдельную задачу: охранная сигнализация, пожарная сигнализация, охранное телевидение и т. д. Все перечисленные системы имеют в своем составе сенсоры, приемно-контрольные приборы, устройства программного управления и т.д. Интеграция сигналов от различных ТСБ осуществляется в данном случае только оператором. Недостатки очевидны. Надежность реагирования системы в целом, вероятность выполнения правильных действий по сигналам и прочие функции системы полностью зависят от внимания и работоспособности оператора — обычно наименее надежного звена системы.

В проектировании ИСБ применяется иной подход. Периферийная часть системы подразделяется на функциональные группы оборудования. Каждая функциональная группа решает одну или несколько смежных технических задач — обнаружение нарушений, контроль прохода, наблюдение за объектами и т. д. Периферийное оборудование рассматривается как источник сигналов, автоматизированная обработка которых является функцией системы в целом. Как правило, далее вся информация от оборудования системы сводится на пункт централизованного наблюдения, где сосредоточен весь «интеллект» ИСБ и размещены рабочие места операторов.

Системы безопасности, создаваемые на базе комплекса ТСБ путем интеграции функций обработки сигналов от периферийной части, программирования общей реакции на события и объединения вывода данных на едином интерфейсе оператора, в современной технической литературе называются интегрированными (ИСБ).

Теоретическое рассмотрение вопроса проектирования ИСБ в общем случае бесполезно, потому что ИСБ, собираемая из унифицированных функциональных элементов, в готовом виде достаточно жестко индивидуально привязывается к объекту. То есть, *свойства объекта практически полностью определяют конечный вид оптимальной для него ИСБ.*

Пример проектирования группировки технических средств ИСБ

Рассмотрим подход к проектированию ИСБ на примере типовой практической задачи. За исходные взяты данные объекта «коттеджный поселок», приведенные в разделе «Обследование объекта».

Структура технических средств ИСБ

Согласно исходным данным, территория объекта составляет несколько квадратных километров. Такая территория не может эффективно наблюдаться с одной точки (особенно в ночное время либо в условиях дождя или снега). Для успешного решения задачи обеспечения безопасности необходимо оборудование территории объекта техническими средствами безопасности. В совокупности ТСБ должны обеспечивать: обнаружение признаков нарушения установленного режима безопасности, передачу сигналов тревоги на ПЦН, определение местоположения и идентификацию нарушителей, целеуказание для задержания нарушителей или противодействия им, запись информации по обстановке и событиям на объекте. ТС, используемые на объекте, состоят из описанных ниже групп оборудования, каждая из которых предназначена для решения определенной задачи. Блок-схема подключения ТСБ и обеспечения дополнительных сервисов приведена на рис. 1(стр.8).

Средства сигнализации

Для обнаружения фактов несанкционированного проникновения на территорию необходимо периметр (внешнее ограждение) оборудовать средствами сигнализации. Наибольшей надежностью функционирования в широком диапазоне погодных условий обладают ТС с подключением по кабелю.

Для установки ТС сигнализации необходима прокладка вдоль внешних ограждений на всем их протяжении кабельных линий питания устройств (220 В) и передачи сигналов. В целях повышения надежности и скрытности работы ТСБ линии должны быть подземными. Поскольку строительство отдельной кабельной канализации для этих линий нецелесообразно, кабели должны укладываться непосредственно в грунт и закапываться. Количество и емкость (число жил) кабелей необходимо выбирать с 2-3-х кратным запасом относительно потребности оборудования, устанавливаемого при монтаже системы. При подключении нового оборудования или модернизации системы во время эксплуатации имеющийся запас позволит избежать земляных работ, порчи внешнего вида участков и дополнительных расходов.

Выбор средств периметровой сигнализации производится, исходя из наибольшей надежности функционирования в любых погодных условиях, минимума затрат на обслуживание и снижения общей стоимости установки при заданном качестве работы. Кроме того, при установке ТСБ на ограждении внешнего периметра, следует учитывать возможность их повреждения или хищения. Средства, конструктивно исполненные в виде отдельных блоков, в особенности имеющие прозрачные части корпуса (видеокамеры, ИК-датчики), подвергаются в этом отношении повышенному риску.

Учитывая вышеизложенное, для защиты основной части периметра следует выбрать средства обнаружения проникновения с кабельными датчиками. **Чувствительные элементы (ЧЭ)** таких ТС имеют вид петель или отрезков кабеля, закрепляемых на ограждении или вблизи него. Вокруг каждого ЧЭ образуется зона обнаружения шириной 0,5 — 3 метра и длиной, равной длине кабеля. ЧЭ подключаются к блокам управления, передающим возникающие сигналы тревоги на ПЦН. Блоки управления размещаются скрытно в соединительных коробках кабелей, проложенных вдоль ограждения. Всего на периметре формируется от 50 до 100 участков, нарушения на которых вызывают передачу сигнала тревоги. По характеру сигнала дежурный может определить место пересечения периметра с точностью до 50 метров и направить патрульную группу.

На тех участках, где невозможно применение кабельных датчиков, следует установить инфракрасные или микроволновые средства обнаружения.

Для обеспечения **охранно-пожарной сигнализации (ОПС)** жилых домов и прочих строений поселка необходимо использовать серийно выпускаемые комплекты оборудования. Предпочтение разумнее оказать системам известных производителей, выбрав одну марку для всех объектов. Установка стандартного оборудования единого производителя упростит и удешевит монтаж и техническое обслуживание оборудования, повысит надежность его функционирования. К оборудованию ОПС по желанию собственников домов могут быть подключены ручные извещатели для подачи сигналов о пожаре и нападении (тревожные кнопки). Все сигналы от оборудования ОПС по линиям связи сводятся на ПЦН к сотрудникам дежурной смены СБ.

Дополнительно на ПЦН должна быть выведена важнейшая информация и сигналы тревоги от ТС инженерной инфраструктуры: трансформаторной подстанции, насосных подстанций водопровода и канализации, газораспределительной станции и т.п.

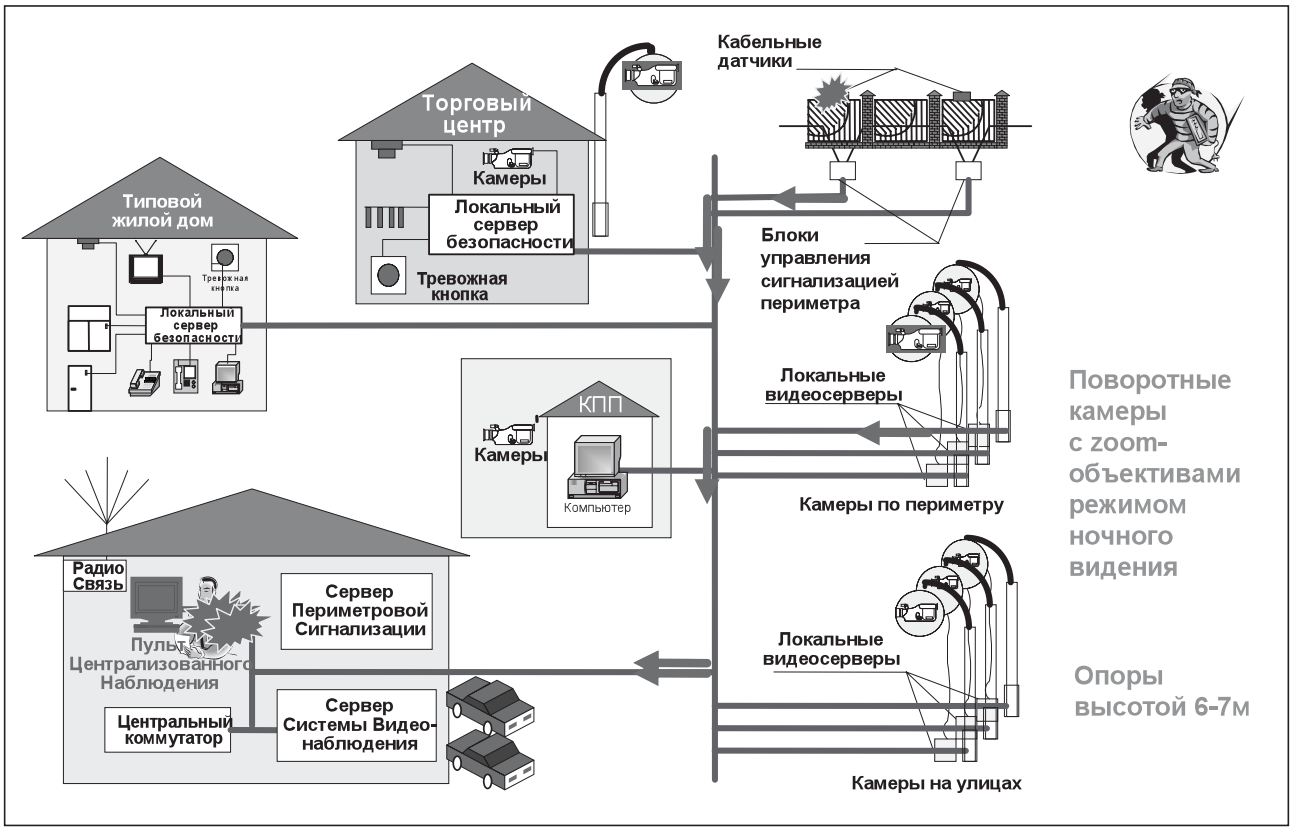

Рис. 2 Сигнализация периметра и телевизионное наблюдение

Средства наблюдения

Для получения информации об обстановке на территории поселка с места расположения дежурной службы и дистанционного наблюдения за обстановкой на месте предполагаемого нарушения территория оборудуется **средствами телевизионного наблюдения (СТН)**.

Желательно, чтобы каждый участок внешнего периметра и внутренней территории в любой момент был доступен для осмотра при помощи СТН. Качество и размеры изображения должны позволять произвести идентификацию человека или транспортного средства. Установки видеокамер на ограждениях следует избегать, поскольку небольшая высота ограждений создает удобные условия для хищения камер. Также обычно неэффективно постоянное наблюдение территории стационарными телекамерами — даже при небольшой площади объекта (несколько квадратных километров) для этого потребуется несколько сотен камер. Большая часть информации, получаемой от них, будет бесполезна для решения задачи обеспечения безопасности.

Оптимальным решением задач наблюдения территории поселка является применение в составе СТН поворотных камер с zoom-объективами (18—24х) и режимом ночного видения. Камеры следует разместить на опорах высотой 6—7 метров, чтобы обеспечить достаточный обзор в условиях плотно застроенной территории. Система СТН строится в два рубежа: внешний — с размещением опор с камерами вблизи внешних углов периметра и внутренний — с размещением опор с камерами в перспективе основных проездов поселка. Камеры, размещаемые на периметре, должны автоматически наводиться на место срабатывания сигнализации. Камеры внутреннего рубежа программируются так, чтобы днем они совершали обзоры территории в заданной последовательности с возможностью ручного перехвата управления, ночью — работали в тревожном режиме от детекторов движения.

Оборудование ПЦН

Состав и функции оборудования ПЦН определяются составом и функциями подключаемого к нему периферийного оборудования. В рассматриваемом случае основные технические системы безопасности, управление которыми интегрируется на ПЦН, следующие:

- периметровая сигнализация;
- система телевизионного наблюдения;
- абонентская ОПС, включая сигнализацию торгового комплекса.

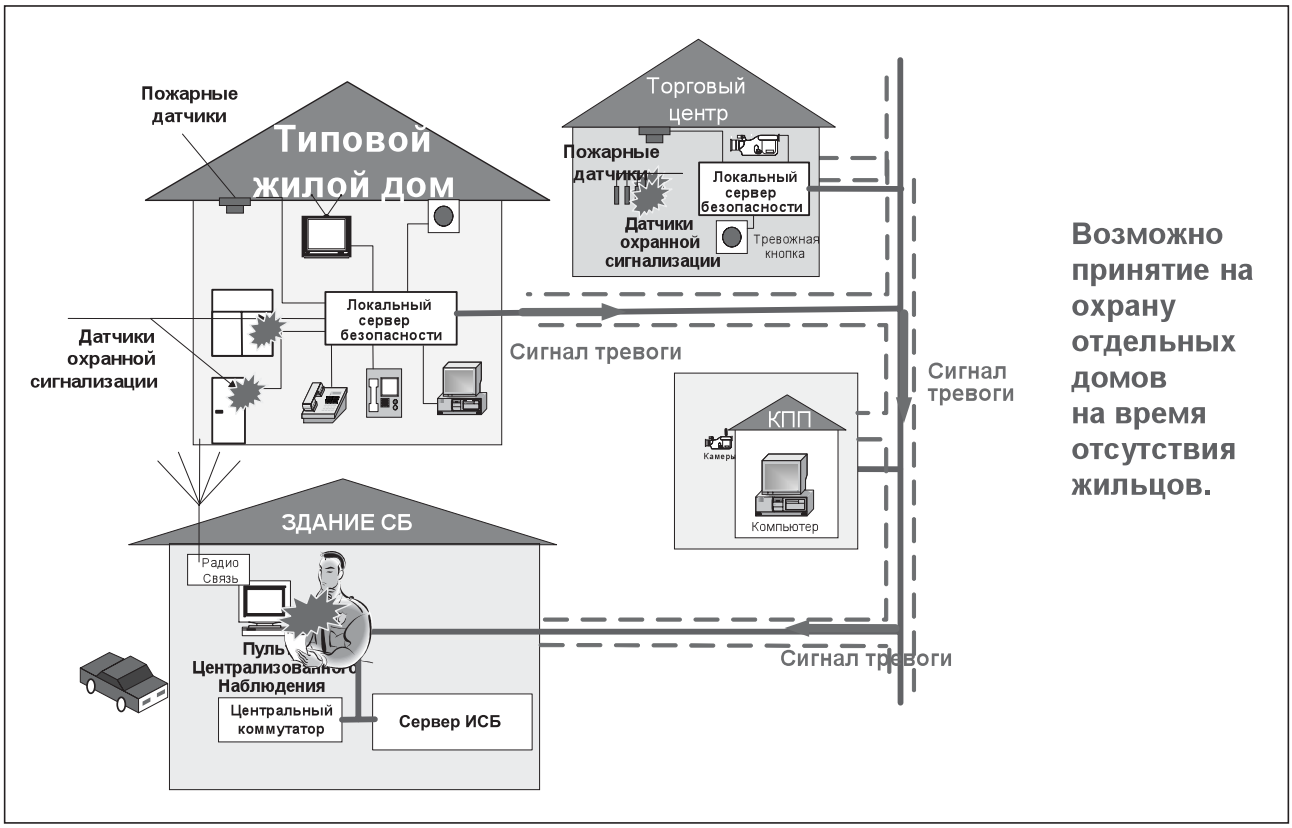

Рис. 3 Пульт централизованного наблюдения

Дополнительно к ПЦН должны быть подключены: приборы сигнализации режимов работы и аварийных состояний инженерной инфраструктуры, системы связи — внутренний телефон, служебная радиосвязь охраны, городской и мобильный телефоны.

ПЦН оборудуется автоматизированной центральной (серверной) частью ИСБ на базе решения, предлагаемого одним из ведущих производителей. В состав оборудования ИСБ включаются центральные блоки периметровой сигнализации, оборудование коммутации телевизионного сигнала и видеозаписи, пульт охранно-пожарной сигнализации зданий.

Сигналы от центральных устройств указанных систем подключаются к группе серверов управления. Информация ИСБ выводится на рабочие места (компьютеры) операторов. Для размещения коммутационного и интегрирующего оборудования должно быть предусмотрено отдельное помещение. Рабочее помещение дежурной службы (операторов ИСБ) обычно снабжается технической мебелью (пультом) для удобного размещения средств отображения и управления ТС и силами СБ.

ПЦН должен быть оборудован централизованной системой бесперебойного электропитания. В систему входят блок питания от аккумуляторов и блок автоматики для подключения питания от автономной генераторной установки в случае длительных перерывов электроснабжения. Питание средств сигнализации и телевизионного наблюдения, установленных на периметре территории, осуществляется от ПЦН.

Средства интеграции отдельных ТСБ в ИСБ

При развертывании ИСБ на территории объекта необходимо организовать прокладку соединительных линий, по которым информация от периферийных ТСБ передается на ПЦН. Для эффективного объединения отдельных ТСБ и функциональных подсистем в единую ИСБ с централизованным сбором информации и управлением подход при решении вопроса о прокладке соединительных линий должен быть системным.

Как показано выше, каждое из ТС безопасности может быть подключено к ПЦН по отдельной линии. В некоторых случаях, когда расстояние до установленного оборудования превышает технические возможности интерфейса, для передачи сигнала необходимо применение промежуточного преобразования. Например, для видеосигнала, пе-

редаваемого по коаксиальному кабелю, это расстояние от камеры до приемного оборудования составляет 200 — 300 м и более. В результате при большом числе установленных ТС схема соединений становится весьма сложной и громоздкой — до нескольких сотен кабелей, входящих на ПЦН, и нескольких десятков блоков преобразования сигналов.

Кабельное оборудование (средства передачи данных)

В условиях, когда количество подключаемого к ПЦН периферийного оборудования превышает несколько десятков устройств, целесообразно рассмотреть решение по организации соединения ТСБ единым кабелем с мультиплексированием потоков данных. Передача разнородных потоков данных от различных ТС по одному кабелю осуществляется за счет преобразования данных к единому цифровому формату. Все подключаемые ТС оснащаются стандартным интерфейсом.

Готовым к использованию техническим решением, отвечающим вышеизложенным требованиям, является **мультисервисная транспортная сеть (МСТС)** на базе оптоволоконного кабеля. МСТС позволяет организовать передачу данных и сигналов управления между периферийными средствами и ПЦН ИСБ по единой для всех устройств сети. Многожильный оптоволоконный кабель МСТС обладает рядом преимуществ перед соединениями ТСБ медным кабелем. Системы передачи данных на базе оптоволоконного кабеля характеризуются:

- большей, по сравнению с проводными системами, емкостью по числу подключаемых устройств;
- намного большими скоростями передачи сигналов;
- высокой долговечностью (десятки лет без замены кабеля и ухудшения свойств);
- меньшей, по сравнению с «медью», стоимостью самого кабеля при одинаковой функциональности системы.

Применение современных технологий проектирования и прокладки оптоволокна во многих случаях позволяет наращивать количество волокон в сети объекта без применения операций сварки волокон и монтажа муфт.

Кабельная сеть МСТС современного технического уровня состоит из собственно кабелей, заложенных в грунт или кабельную канализацию, оптического кросса, размещаемого обычно вблизи ПЦН и абонентских окончаний, выполненных в виде уличных или размещенных в домах соединительных коробок. Все виды периферийного оборудования подключаются к стандартным оптическим разъемам в соединительных коробках. Таким способом все сигналы от оборудования ИСБ приводятся на оптический кросс ПЦН.

Услуги безопасности, предоставляемые по МСТС

Технические средства СБ должны предусматривать возможность принятия на охрану отдельных домов поселка на время отсутствия жильцов. Монтаж ОПС в домах обычно проводится за счет владельцев и согласно их пожеланиям. С целью обеспечения совместимости оборудования и заданного уровня качества обслуживания подключение ОПС в домах к ПЦН должно осуществляться только технической группой СБ. За пользование услугой технической охраны целесообразно взимать с владельцев домов абонентскую плату. ОПС частного дома или сооружений служебного и общественного назначения соединяется с ПЦН через микропроцессорный блок управления, монтируемый в каждом из подключаемых зданий.

Дополнительные возможности МСТС

МСТС современного технического уровня, построенная на базе многожильного оптоволоконного кабеля, имеет значительный запас по емкости и производительности, относительно потребностей оборудования ИСБ. Технические характеристики МСТС позволяют подключить к ней одновременно все электронное оборудование, установленное на территории объекта.

С помощью МСТС может быть дополнительно организовано:

- подключение местной и городской телефонной связи;
- прямая связь абонентов с ПЦН для передачи экстренных сообщений;
- дистанционное управление инженерным оборудованием дома;
- дистанционный учет потребления электроэнергии, воды и т.д.;
- подключение к сети Интернет и сервисам сети передачи данных поселка;
- распределение телевизионных программ (до 200 программ по одному волокну);
- доступ к услуге «видео по запросу»;
- прочие сервисы.

Перечень сервисов, реализация которых возможна с помощью оборудования и технологии МСТС, превосходит возможности сетей, прокладываемых отдельно для предоставления каждой из перечисленных услуг. Функции удаленного управле-

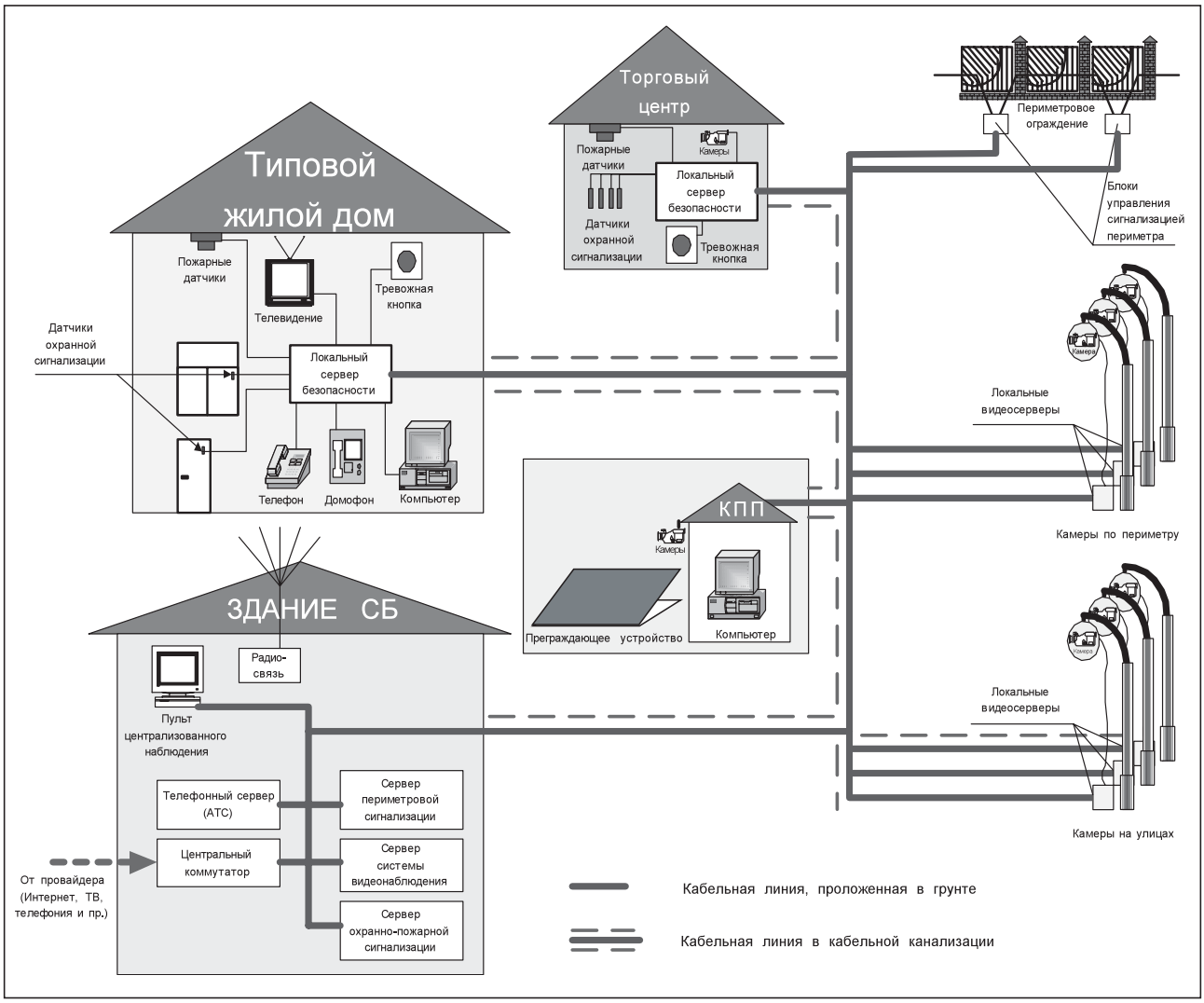

Рис. 4 Типичная схема подключения ТС безопасности и обеспечения дополнительных сервисов

ния инженерным оборудованием расширяют возможности дистанционного контроля безопасности зданий на территории поселка.

Более подробно технические возможности и функции МСТС рассматриваются в Приложении 1.

Работа с ИСБ

Из всего вышеизложенного понятно, что установку и конфигурирование ИСБ должны выполнять специалисты высокой квалификации. К субподрядным организациям, выполняющим работы по оборудованию территории кабельными линиями, также предъявляются достаточно жесткие требования. С другой стороны, высокая автоматизация и предварительное программирование реакции ИСБ на различные сигналы и ситуации делают простой и удобной работу оператора системы и дежурной смены службы безопасности.

В случае возникновения тревоги от одного из датчиков, подключенных к системе, на место тревоги или подходы к нему наводится ближайшая из телекамер. Изображение выводится на специальный «тревожный» монитор, который в обычное время выключен. Параллельно с привлечением внимания оператора ИСБ начинает запись событий с запрограммированных камер на видеорегистраторе, добавив несколько предшествующих тревоге минут из буфера. Одновременно включаются сигналы оповещения и исполнительные устройства: освещение, приводы замков, дверей, ворот, изготавливается к действию противопожарная система (если тревога возникла от пожарного датчика). Вместе с сигналом тревоги оператору может быть предъявлена заранее разработанная инструкция по действиям в сложившейся ситуации. Если заранее запрограммировано, то отправляется сигнал тревоги во внешние

службы: пожарную охрану, орган МВД, охранное предприятие и т.п.

С помощью средств ИСБ оператор может контролировать и протоколировать действия сотрудников СБ, занятых принятием мер по тревоге, обнаруживать нескольких одновременно действующих нарушителей.

Если в составе ТСБ объекта кроме ТС, упомянутых в примере, есть еще система контроля и управления доступом СКУД, действие программ, автоматизирующих действия ИСБ, распространяется и на эту подсистему. В зависимости от поступающих сигналов и запрограммированных реакций СКУД может: изменить правила доступа в помещения, заблокировать проходы или проезды на территории, проследить перемещение через считыватели карточки с заданным номером и т.д.

Технические средства ИСБ поддерживают полный комплекс мероприятий по обеспечению безопасности объекта, начиная от обнаружения нарушения режима до принятия мер по его ликвидации. Данные, накопленные ИСБ, доступны в течение длительного времени (ограниченного только размерами памяти сервера) для анализа защищенности объекта и разбора произошедших инцидентов.

Типичная схема подключения ТС безопасности и обеспечения дополнительных сервисов.

Организация бесперебойного электропитания

Для надежной работы ИСБ очень важна надежность электропитания. На большинстве защищаемых объектов наиболее целесообразно применение централизованной схемы организации системы бесперебойного электропитания. В примере, рассмотренном выше, в качестве источника гарантированного питания была выбрана **автономная генераторная установка (АГУ)**. На АГУ, в случае отключения основной линии электроснабжения объекта, должны быть переключены потребители электроэнергии, для которых недопустим перебой питания в более чем 10 — 20 минут. Для повышения надежности в составе АГУ используются два одинаковых генератора суммарной мощностью в 1,3 — 1,5 раза больше, чем суммарная мощность потребителей, запланированных для бесперебойного электропитания.

Расчетное время восстановления электропитания при запуске генераторов из выключенного состояния составляет несколько десятков секунд. Потребители, для которых вообще недопустим перерыв электроснабжения (сигнализация, компьютерное оборудование и т.п.), должны в течение этого времени питаться от аккумуляторных источников бесперебойного питания. Здесь необходимо сделать важное практическое замечание: СБ объекта должна контролировать состояние и готовность к использованию агрегатов резервного электропитания и запаса топлива к ним.

Дополнительные средства службы безопасности

Современные ИСБ общего назначения не снабжаются исполнительными устройствами, позволяющими задержать нарушителя или причинить ему повреждения. Кроме того, в ряде случаев такие действия запрещены законодательно. Это главная причина, по которой проектировщик системы должен хорошо представлять себе силы и средства, взаимодействующие с ИСБ. В противном случае заказчик будет вправе упрекнуть подрядчика в создании «дорогой игрушки», которая никак не повысила реальную безопасность объекта. Поэтому, предлагая концепцию или проект ИСБ, следует обязательно включать в нее раздел о средствах обеспечения работы СБ. Эти средства позволят избежать появления слабых мест в цепочке действий от сигнала тревоги до момента принятия мер к нарушителям.

Назовем некоторые наиболее важные из дополнительных средств.

Средства связи

Сотрудников СБ объекта и операторов ПЦН целесообразно снабдить мобильными средствами радиосвязи в высоконадежном всепогодном исполнении, работающими на одном или двух фиксированных частотных каналах. Разумной мерой является закрытие канала связи (скремблирование).

Обеспечение проездов и проходов к объектам охраны, периметру

Реакция СБ на нарушения режима безопасности требует быстрого прибытия сотрудников к месту происшествия. С учетом численности патрульной службы (одна группа из двух человек) необходимо обеспечить возможность их прибытия в необходимую точку территории и периметра поселка не более чем за 2 — 3 минуты. Применение транспортных средств решает задачу сокращения времени прибытия и сохранения сил сотрудников СБ для противодействия нарушителям.

В условиях размещения объекта в пригородной зоне для охраны периметра необходима подготовка маршрута патрулирования снаружи ограждения по всей его длине. Желательно, чтобы профиль

Рис. 5 Такой забор не является преградой для злоумышленников

маршрута естественным образом препятствовал движению по нему постороннего автотранспорта. Обычно достаточно освободить от деревьев и кустарниковой растительности полосу шириной до 10 метров, считая от ограждения. В лесу вдоль основного и дополнительного периметра необходимо сформировать просеки такой же ширины. Для стока воды по внешнему краю полосы прокопать канаву.

Если часть территории объекта продана в частное владение, необходимо включить в договор администрации объекта с собственниками участков административное обеспечение действий охраны. В том числе должен быть разрешен проход сотрудников СБ через участки к периметру в случае необходимости предотвращения нарушений безопасности и для осмотра ТС сигнализации (если другим способом это сделать невозможно).

Средства физической защиты. Фортификационные сооружения

Средства физической защиты предназначены для повышения эффективности работы сотрудников СБ и затруднения проникновения нарушителей на защищаемый объект. Охраняемый объект целесообразно окружить заграждением (забором). Форму полотен заграждения следует выбирать, исходя, прежде всего, из их защитных свойств. Примером хорошо продуманного забора является решетка Летнего сада в Санкт-Петербурге: с одной стороны, это всемирно известный архитектурный шедевр, с другой — через нее очень непросто перелезть.

Для практического выбора конструкции ограждения есть очень простой критерий — задумайтесь, насколько быстро и с помощью каких средств, вы сами могли бы его преодолеть. На фотографиях приведены: наиболее типичная ошибочная конструкция заграждения (рис. 5) и образец конструкции, отвечающей основному назначению, предлагаемый одним из поставщиков компании «Инфосистемы Джет» для установки на объектах (рис. 6).

Для затруднения действий нарушителей целесообразно усилить ограждения контролируемой территории объемной металлической спиралью типа «Егоза», закрепленной на укосинах от верха ограды внутрь территории. Спираль может быть окрашена в тон основного заграждения. Дополнительное заграждение «Егоза» значительно затруднит нарушителю преодоление периметра или потребует наличия у него заранее подготовленных специальных режущих инструментов. Предлагаемая доработка, возможно, ухудшит внешний вид существующего ограждения, но в несколько раз увеличит время, необходимое нарушителю для его преодоления.

Основной въезд на объект следует оборудовать управляемым преграждающим устройством тяжелого типа, рассчитанным на сдерживание попытки прорыва створа ворот грузовым автомобилем.

Средства транспорта

Для обеспечения своевременного прибытия патрульной группы к месту нарушения режима безопасности, объезда удаленных участков периметра и преследования нарушителей на территории объек-

Рис. 6 Несмотря на кажущуюся простоту такого ограждения, преодолеть его очень трудно

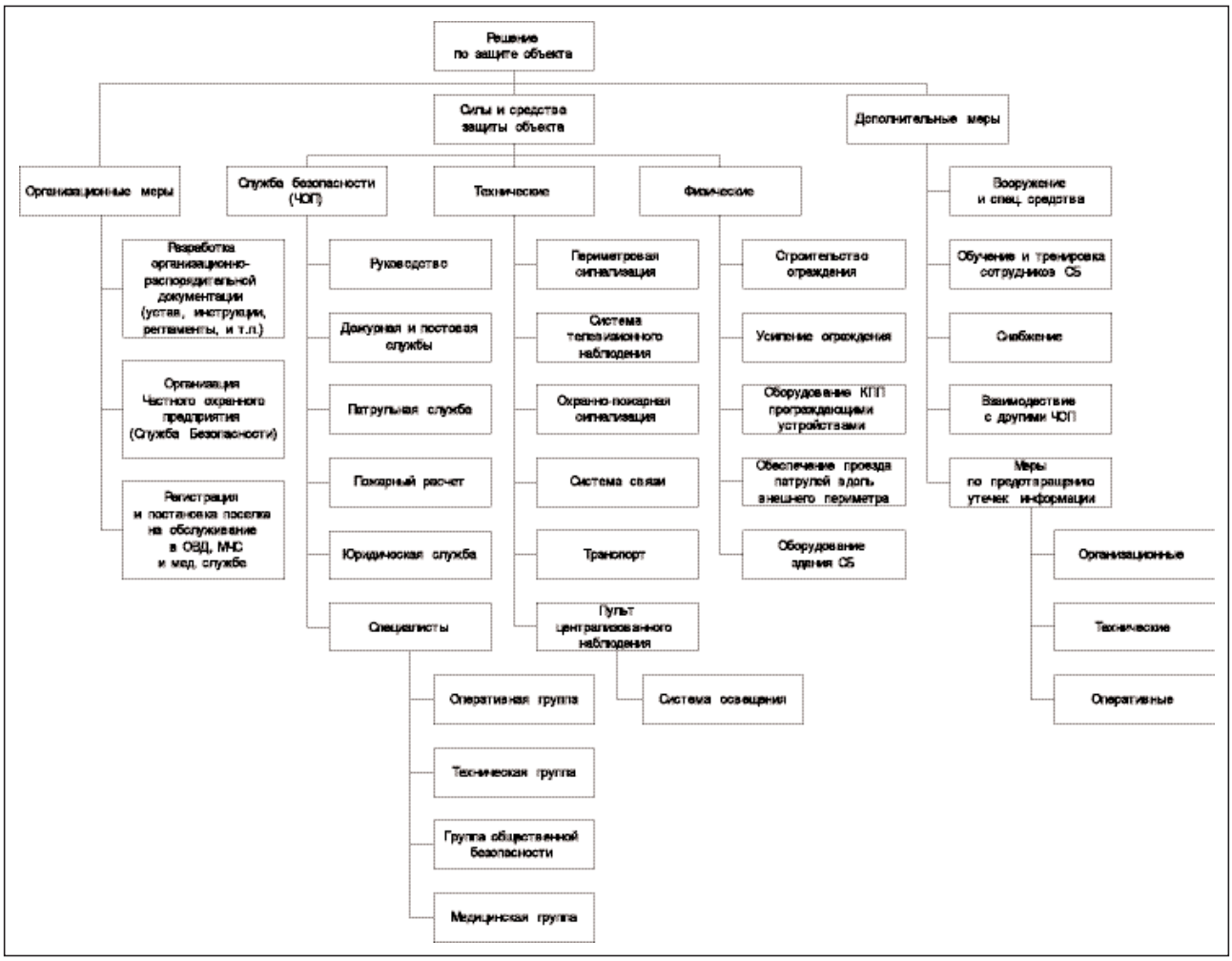

Рис. 7 Примерная структура решения по защите типового объекта «Жилой поселок с собственной службой безопасности». Такую общую схему полезно составить для наглядности, оценки полноты и взаимной координации запланированных мероприятий по защите объекта с применением ИСБ.

та необходимо снабжение СБ несколькими единицами маневренного вездеходного транспорта.

Для обеспечения работы по эксплуатационному обслуживанию, реконфигурации и ремонту технических средств, а также для решения некоторых оперативных задач целесообразно предоставить службе безопасности микроавтобус повышенной проходимости с грузовым отсеком и площадкой на крыше. С его помощью будет доставляться на периметр территории приборное оборудование, необходимое для настройки сигнализации, осуществляться доступ к высоко расположенным телекамерам, скрытое наблюдение по временной схеме на некоторых участках территории, а в экстренных случаях с помощью этого микроавтобуса доставить задержанных нарушителей в местные органы внутренних дел.

Помещение

Для эффективной работы СБ (причем на крупных объектах обязательно) следует предусмотреть строительство специализированного здания. Обычно это каменный двухэтажный дом с остекленной надстройкой над вторым этажом для размещения операторских мест ПЦН и работающей на них дежурной службы. Здание СБ должно быть снабжено металлическими дверями, окна — защищены решетками или в них должны быть установлены особо прочные (бронированные) стеклопакеты. Одно из помещений целесообразно оборудовать под «комнату ожидания» для временного пребывания задержанных нарушителей. На здании следует оборудовать открытую наблюдательную позицию (балкон, остекленный фонарь). Непосредственное визуальное наблюдение за объектом повышает надежность несения службы дежурной сменой. Общая полезная площадь здания для 50 человек должна составлять 800 — 1000 м^2.

В первом этаже здания оборудовать гараж на два машиноместа для обслуживания транспортных средств СБ. Здание должно находиться недалеко от основного въезда на территорию. К нему необходимо проложить линии инженерной инфраструктуры

и слаботочной канализации (16х100) от ближайшего разветвительного колодца.

Применение ИСБ на объектах промышленности и транспорта

Рассмотренный выше пример охраняемого объекта совершенно не исчерпывает области применения ИСБ. Общий принцип построения интегрированной системы позволяет расширить территорию, обслуживаемую одной системой, до квазиглобального масштаба, например, включив в одну ИСБ объекты промышленной корпорации, распложенные на разных континентах. ИСБ может быть применена на объекте любой сложности, территориальной конфигурации и назначения. Средствами ИСБ можно защищать подвижные объекты и их группировки. Единственным принципиальным требованием для организации ИСБ является наличие каналов связи заданной надежности и производительности между комплектами оборудования, входящими в единую систему.

Типовыми конфигурациями объектов, нуждающихся в интегрированной системе безопасности, можно назвать:

- офисное здание среди городской застройки, занимаемое одной или несколькими организациями;
- территорию промышленного предприятия;
- складской объект;
- жилой массив в городской застройке, как правило — многоэтажный;
- жилой массив за городом, как правило — малоэтажный с озелененной территорией;
- отдельно расположенный дом со службами типа «усадьба» (относительно редко, но встречается).

Для перечисленных объектов задача проектирования ИСБ решена специалистами в общем виде. Вопрос адаптации решения к конкретному объекту заключается лишь в его количественном масштабировании. Технологическая цепочка от проектирования до сдачи работающей системы заказчику включает следующие этапы:

- аудит текущего состояния системы безопасности объекта — предпроектное обследование;
- подготовка концепции обеспечения безопасности объекта;
- защита концепции, формирование и утверждение технического задания на систему;
- разработка рабочей и проектно-сметной документации на систему;
- монтажные и пусконаладочные работы;
- обучение персонала заказчика и опытная эксплуатация системы;
- сдача ИСБ в рабочую эксплуатацию.

В зависимости от масштаба объекта и объема проводимых работ, некоторые этапы могут быть совмещены или проработаны более подробно. В любом случае «под монтаж» система будет проработана «до гаек». На практике, особенно часто в последнее время, встречаются задачи по созданию технических систем обеспечения безопасности для объектов, имеющих нестандартную конфигурацию. Здесь можно выделить два типа объектов:

- распределенные объекты, масштаб которых сопоставим с территорией государства;
- нечетко ограниченные объекты типа районов большого города.

При анализе новых задач методика проектирования ИСБ была расширена с сохранением основного подхода — построение индивидуальной системы для каждого защищаемого объекта и решаемой задачи из готовых блоков со стандартной функциональностью. Во всех случаях функциональным ядром ИСБ является МСТС с набором стандартных интерфейсов.

Для территориально распределенной ИСБ разработано решение с логической МСТС (**ЛМСТС**) в виде **виртуальной частной сети (VPN)**, наложенной на собственные или арендуемые заказчиком каналы дальней связи. Для служб масштаба города разрабатывается гибридное решение в виде нескольких логических сетей, наложенных на выделенную физическую сеть и каналы городских операторов связи в местах отсутствия выделенной сети.

Приведем пример разработки концепции территориально распределенной ИСБ с ограниченной функциональностью. Заказчик — крупная авиакомпания, имеющая собственный парк самолетов и сеть пассажирских и грузовых терминалов по всей территории России. Далее приведены фрагменты текста документов, характеризующих принципы подхода специалистов к решаемой задаче.

Согласно техническому заданию, система должна обеспечивать видеонаблюдение территории, зданий, помещений и иных объектов воздушного и прочего транспорта, в том числе подвижных объектов и их составных частей. Перечень зон и условий наблюдения задается частным техническим заданием, формируемым для каждого технологиче-

ского **комплекса транспорта (КТ)** или **транспортного средства (ТС)**.

В системе должны быть реализованы функции детектирования движения, распознавания и сопровождения объектов с передачей соответствующей информации оператору, а также автономное видеонаблюдение в каждом КТ или отдельном ТС, которое должно осуществляться функционально законченным комплектом средств **системы промышленного видеонаблюдения (СПВ)**.

Законченный комплект средств СПВ должен обеспечивать выполнение следующих функций:

- преобразование изображения наблюдаемой сцены в электрические сигналы с помощью видеокамер во всем диапазоне условий наблюдения, существующем на объектах развертывания;
- запись и хранение получаемых от видеокамеры сигналов на физическом носителе информации;
- поддержку интерфейсов с оператором, к которым могут быть подключены средства воспроизведения видеосигнала, поступающего в реальном времени и в записи, а также средства управления комплексом;
- программное управление комплектом с часами реального времени, памятью команд и возможностью управления по сценарию (расписанию);
- поддержание системного интерфейса для стыковки с другими комплексами СПВ, построенного на базе открытой модели сетевых взаимодействий (OSI).

Комплексы, монтируемые на подвижных объектах, должны иметь беспроводной системный интерфейс.

Система в целом должна обеспечивать:

- обмен видео и иной необходимой информацией между комплексами, установленными на различных КТ и отдельных ТС (в том числе возможность передачи информации с ТС через комплект оборудования КТ, на территории которого в данный момент находится ТС);
- обмен информацией между отдельными устройствами, входящими в функционально законченный комплекс системы по цифровой магистрали с логической архитектурой «сегментированная шина», со скоростью передачи данных не ниже 1 Гбит/с для основной магистрали комплексов, монтируемых на стационарных объектах, и не ниже 100 Мбит/с для комплексов, монтируемых на подвижных объектах;
- защиту обрабатываемой информации и каналов обмена информацией, выходящих за пределы территории КТ.

Блочно-модульное построение отдельных комплектов и системы в целом должно обеспечивать техническую возможность подключения дополнительных устройств в составе комплекса и новых комплексов в систему без перерыва в работе действующей части системы.

В данном случае предлагается решение: территориально распределенная ИСБ с ограниченной функциональностью — только функции видео и тревожное оповещение. Система строится на базе ЛМСТС, имеющей беспроводные окончания. Защита ЛМСТС выполняется по полнофункциональной схеме (см. Приложение 2).

Технический уровень предлагаемой ИСБ характеризуется следующими данными:

- широкое распространение видеокамер с внутренней цифровой обработкой изображения;
- использование для передачи изображений от камеры до средств обработки и/или записи цифровых линий связи;
- использование цифровых интерфейсов для управления функциями видеокамер;
- широкое распространение на объектах транспорта локальных вычислительных сетей с высокими скоростями передачи данных (до 10 Гбит/с);
- стандартизация интерфейсов и протоколов передачи данных, встраиваемых в оборудование, с ориентацией на использование в качестве среды передачи данных единой объектовой ЛВС;
- использование технологий интеллектуальной обработки изображений, позволяющей строить сложные многозональные детекторы движения, производить опознание объектов по базе данных и осуществлять слежение за объектом, перемещающимся по сложной траектории;
- применение в составе системы обрабатывающих центров высокой производительности, пригодных для решения задач опознавания лиц, предсказания перемещений объектов и верстки изображений с нескольких видеокамер на один экран.

Основные свойства архитектуры системы:

- блочно-модульное построение системы в целом и отдельных комплектов должно обеспечивать техническую возможность подключения дополнительных устройств в составе комплекса и новых комплексов в систему без перерыва в работе действующей части системы;
- в концепцию построения СПВ ОВТ заложен территориально распределенный принцип построения с равноправными сетевыми узлами;

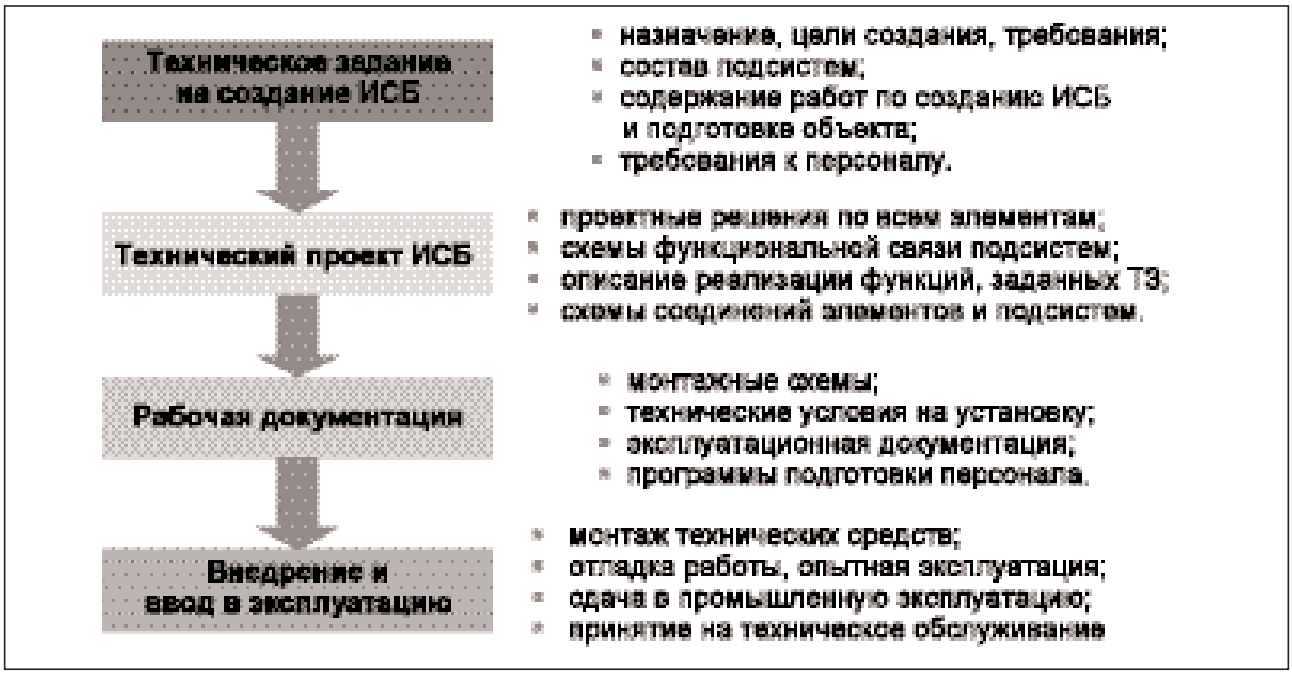

Рис. 8 Стадии реализации проекта ИСБ

- сетевая модель взаимодействия должна предусматривать маршрутизацию сообщений с передаваемой от узла к узлу информацией в едином адресном пространстве;
- в проект СПВ заложены требования к подсистеме информационной безопасности (ПИБ) СПВ как системе, имеющей стык с каналами связи общего пользования.

Проектирование и реализация ИСБ, построенной согласно положениям разработанной концепции, полностью отвечает принципу применения только передовых технических решений.

Технический уровень и жизненный цикл ИСБ

ИСБ обычно рассчитываются на длительный срок эксплуатации. Без замены основного оборудования он может составлять до 10 лет. Коммутирующее оборудование МСТС может служить до 15 лет, а кабельная инфраструктура 40 — 50 и более лет. Поэтому ради сохранения вложений (защиты инвестиций) заказчика для ИСБ должно выбираться оборудование передового технического уровня.

В ближайшей перспективе такой уровень смогут обеспечить:

- переход к полностью оптоволоконным кабельным сетям передачи данных;
- применение беспроводного оборудования передачи данных на базе протокола 802.11;
- появление универсального периферийного видео-сервера для обслуживания профессиональных камер наблюдения с высоким качеством оптики;
- совершенствование технологии распознавания образов.

Архитектура ИСБ, построенной на базе МСТС с набором стандартных интерфейсов, позволяет в процессе эксплуатации проводить частичную замену оборудования. При этом вся система, кроме непосредственно заменяемого оборудования, остается в рабочей эксплуатации. Реконфигурация системы после замены оборудования проводится на программном уровне также без остановки оборудования.

Заключение

Некоторые перспективные свойства ИСБ, или о чем часто спрашивают

Стык ИСБ с системами информационной безопасности. Возможен. Требует разработки стыковочного программного модуля.

Автономная подвижность исполнительных устройств ИСБ (электронный охранник). Возможна. До образцов, показанных в фильме «Терминатор», им

пока далеко, но устройства на колесном и гусеничном шасси, снабженные телекамерами и стрелковым оружием, уже проходят опытную эксплуатацию в некоторых «горячих точках» планеты (не у нас).

Свобода в принятии решений. Ограниченно возможна, базируется на функциях искусственного интеллекта. Полезна для больших территориально распределенных систем, требует наличия в составе системы обрабатывающего сервера высокой математической производительности.

Периферийные устройства особо малого размера (нанотехнологические). Возможны. Очень дорогие и только импортные, требуют доработки стандартных интерфейсов для обмена информацией.

Краткие выводы

Итак, для построения ИСБ современного технического уровня, эффективной по критерию «цена — качество», НЕ СЛЕДУЕТ:

- применять оборудование, имеющее только локальные функции;
- применять оборудование, не имеющее стандартного цифрового интерфейса для передачи данных и управления функциями;
- применять оборудование и системы, работа которых не может отображаться и управляться стандартными средствами графического интерфейса персонального компьютера;
- применять системы и оборудование, не имеющие четкого технического описания команд и состояний устройств.

Все это сразу сделает систему устаревшей.

Потенциальному заказчику НЕОБХОДИМО:

- представить себе — что и от чего он хочет защищать;
- изложить задачу специалистам;
- уметь сравнить и оценить предлагаемые решения;
- выбрать наиболее подходящий проект.

Связаться с автором можно по адресу: besedin@jet.msk.ru

Приложение 1

Мультисервисная транспортная сеть (МСТС) для ИСБ. Основные положения

На основе данного документа может быть разработано техническое задание для оснащения МСТС объекта (совокупности объектов) заказчика. Конфигурация МСТС ориентирована на развертывание на ее технической базе объектовой ИСБ.

Общие сведения

Для интегрированной системы безопасности охраняемого объекта **мультисервисная транспортная сеть (МСТС)** является единым решением, обеспечивающим надежной высокоскоростной цифровой связью все технические средства ИСБ. Рекомендуемые настоящим Приложением технические решения позволяют обеспечить построение надежной универсальной, масштабируемой и экономически эффективной сетевой инфраструктуры связи.

А.1.1 Назначение МСТС

Мультисервисная транспортная сеть является опорной технической системой, предназначенной для передачи разнородных данных от различных независимых подсистем: безопасности, управления технической инфраструктурой объекта, организации телефонной связи, доступа в Интернет, распределения телевизионных программ и др.

А.1.2 Общие требования к МСТС

Мультисервисная транспортная сеть должна обеспечивать:

- подключение технических средств безопасности, устанавливаемых на территории объекта, к пульту централизованного наблюдения;
- транспортный уровень для работы подсистем:
  - локальной сети передачи данных,
  - телефонии,
  - доступа в Интернет,
  - распределения телепрограмм.

МСТС должна обеспечивать качество услуг и надежность/доступность в соответствии с требованиями наложенных подсистем.

В МСТС должен быть заложен запас по пропускной способности и производительности, чтобы при необходимости можно было ввести в эксплуатацию дополнительные подсистемы.

Технические решения, применяемые для построения МСТС

1. Технология «оптического» Ethernet

Для построения МСТС выбрана технологию Ethernet с передачей данных по оптоволоконному кабелю.

Основные достоинства данной технологии — высокая производительность, удобная масштабируемость сети, унификация подключения периферийных устройств и высокая управляемость сетевой инфраструктуры.

Технология Ethernet является динамично развивающимся, но в то же время прочно устоявшимся стандартом. Использования технологии «оптического» Ethernet заметно увеличивает экономическую эффективность затрат на сооружение МСТС.

Технология Ethernet в МСТС используется «сквозным образом» — для подключения персональных компьютеров пользователей к локальной сети и для подключения серверов и организации соединений между коммутаторами в локальной сети. За счет сквозного использования одного протокола достигается эффект «прозрачности» сети — работа конечных пользователей происходит так, как будто они непосредственно подключены к серверам потребляемых услуг.

На настоящий момент существует возможность использования технологии Ethernet в сетях операторов связи до масштаба города включительно — для организации соединений между локальными сетями клиентов. Все преимущества технологии «оптического» Ethernet могут быть использованы для построения МСТС любого территориально распределенного объекта.

Преимущества используемой технологии

Простота подключения абонентских устройств
При использовании технологии «оптического» Ethernet со стороны клиента для подключения к распределенной сети нужен только свободный порт Ethernet на коммутаторе. Нет необходимости в установке дополнительного устройства доступа. За счет уменьшения количества используемого оборудования и технологий уменьшаются затраты клиента на установку оборудования и его дальнейшее техническое сопровождение.

Эффективность использования канальных ресурсов и производительность
Оборудование с оптическими интерфейсами Ethernet с пропускной способностью до 1 Гбит/с широко представлено на рынке телекоммуникационных устройств. Ведущие производители оборудования предлагают оборудование с оптическими интерфейсами Ethernet 10 Гбит/с.

При подключении клиентов к сети оператора с использованием технологии «оптического» Ethernet на каждое соединение может быть выделена пропускная способность от 1 до 100 Мбит/с без замены оборудования и до 1 Гбит/с при наличии соответствующего порта со стороны локальной сети.

Технологичность решения для оператора МСТС

С точки зрения оператора сети технология «оптического» Ethernet привлекательна своими возможностями по простоте разделения трафика различных пользователей. Технология «оптического» Ethernet позволяет обеспечить передачу трафика данных различных подключенных пользователей (подсистем) на уровне Ethernet, без осуществления его маршрутизации в сети оператора. Технология позволяет обеспечивать возможность построения наложенных сетей с собственной, независимой адресацией. Универсальная транспортная сеть типа МСТС может быть использована оператором для одновременной и независимой передачи данных различных технических систем.

2. Архитектура МСТС

В структуре МСТС выделяются следующие элементы:

- **Линейные сооружения** — кабельные трассы, кабели, пассивные распределительные устройства. Линейные сооружения обеспечивают среду передачи сигналов активного оборудования транспортной сети.
- **Магистральные узлы** — высокопроизводительное, надежное ядро мультисервисной транспортной сети. Магистральные узлы обеспечивают сбор трафика абонентских узлов доступа и его передачу до центрального узла сети или до других абонентских узлов доступа. Магистральные узлы должны оставаться работоспособными вне зависимости от состояния (включения/отключения) абонентских устройств.
- **Абонентские узлы доступа** — устройства, устанавливаемые на территории участка (коттеджа) абонента. Абонентские узлы обеспечивают подключение к МСТС устройств абонента и оконечных устройств наложенных подсистем.

Линейные сооружения
В качестве основы линейных сооружений предлагается использовать проложенные в кабельной канализации линии оптоволоконного кабеля, обладающие рядом преимуществ по сравнению с другими линиями связи (радио, медными, коаксиальными), включая высокую пропускную способность, надежность, защищенность от внешних воздействий электромагнитного характера, технологичность.

Магистральные узлы
В качестве магистральных узлов предлагается использовать универсальные коммутаторы модульной конструкции, поддерживающие:

- передачу разнородного трафика по оптическим линиям связи,

- различные топологии межузловых соединений, обеспечивающие наличие резервных путей передачи трафика в случае возникновения аварийных ситуаций на линейных сооружениях и неисправностях отдельных узлов магистральной сети,
- механизмы автоматического резервирования наиболее критичных компонентов,
- подключение нескольких абонентских узлов доступа,
- полнофункциональное удаленное управление и мониторинг.

Модульные магистральные узлы позволяют наращивать количество поддерживаемых абонентских подключений по мере необходимости.

В качестве магистральных коммутаторов могут быть использованы стоечные коммутаторы технологии, поддерживающие технологию Optical Ethernet. Коммутаторы соединяются между собой в кольцевые или древовидные топологические структуры с использованием интерфейсов Gigabit Ethernet или 10 Gbit Ethernet. Для подключения абонентских устройств доступа используются порты Fast Ethernet или Gigabit Ethernet.

Абонентские узлы доступа

В качестве оборудования абонентских узлов доступа к МСТС используются коммутаторы Ethernet, поддерживающие:

- подключение абонентских оконечных устройств и оконечных устройств наложенных сервисных подсистем с использованием интерфейсов Ethernet и Fast Ethernet,
- подключение к узлам магистральной сети с использованием оптических портов Fast Ethernet и/или Gigabit Ethernet,
- полнофункциональное удаленное управление и мониторинг.

3. Сервисные подсистемы

Передача данных наложенных систем

К наложенным на МСТС системам передачи данных в первую очередь относятся интегрированная система безопасности и система управления инженерной инфраструктурой объекта. Обе указанные системы являются критически важными для объекта. Оконечные устройства наложенных подсистем, в зависимости от места их размещения, могут подключаться как к абонентским, так и к магистральным узлам МСТС.

Возможности МСТС позволяют подключать ТС указанных систем в любом месте территории объекта. Сбор передаваемой информации и управление системами обеспечивается в одной или нескольких заданных проектом точках путем подключения к МСТС — пульта централизованного наблюдения, централизованной диспетчерской коммунального хозяйства и т.д.

Телефонная связь

Для обеспечения абонентов услугами телефонии на центральном узле МСТС устанавливается цифровая АТС, обеспечивающая:

- развертывание или модернизацию внутренней телефонной сети объекта с собственным номерным пространством;
- подключение телефонной сети объекта к городской телефонной сети общего пользования с возможностью предоставления абонентам «прямых» городских телефонных номеров;
- поддержку экономичных каналов междугородней и международной связи на основе IP-телефонии.

Подключение стандартных телефонных аппаратов к абонентским узлам МСТС осуществляется через недорогие цифроаналоговые адаптеры. Подключение цифровых абонентских телефонных аппаратов (IP-телефонов) с расширенной функциональностью осуществляется напрямую к порту абонентского узла МСТС.

Подключение к Интернет

Подсистема доступа к Интернет является одной из наложенных на МСТС сервисных подсистем. Коммутатор центрального узла МСТС обеспечивает подключение к сети или сетям операторов услуг доступа к Интернет (провайдеров). Абонентские устройства (персональные компьютеры, ноутбуки, коммуникаторы и т.п.) подключаются непосредственно к портам Ethernet/Fast Ethernet абонентских узлов доступа МСТС.

Телевидение

Подсистема распределения телевизионных программ может быть наложена на МСТС объекта двумя способами, различающимися сервисными возможностями и деталями технической реализации.

По первому варианту у абонента устанавливается специализированное устройство доступа к услугам цифрового телевидения (Set Top Box), которое подключается к МСТС с использованием интерфейса Fast Ethernet и через стандартный видеовход подключается к телевизору абонента. Подключение к услугам цифрового телевидения с использованием специализированного устройства позволяет обеспечить предоставление дополнительных серви-

сов, таких как видео по запросу, персональный телетекст и пр.

При подключении телевизоров абонента с использованием антенного входа телевизора (2-й вариант) на абонентском узле устанавливается оптический модем кабельного телевидения. Модем кабельного телевидения подключается с использованием отдельных волокон оптического кабеля к центральному узлу кабельного телевидения. Такая схема позволяет абоненту просматривать пакет телевизионных каналов, которые передаются в МСТС от провайдера телекоммуникационных услуг (например, КОМКОР-ТВ). При втором варианте подключения более простым и, следовательно, дешевым получается центральное устройство распределения телевизионных программ МСТС.

Заключение

Основные свойства МСТС как технического решения, применяемого в качестве опорной сети связи объекта, следующие.

1. Техническое решение в виде опорной МСТС, использующей технологию «оптический» Ethernet, по своим характеристикам полностью удовлетворяет потребностям технических систем ИСБ.
2. МСТС строится на базе однотипных многожильных оптоволоконных кабелей, не более двух на каждом направлении связи.
3. Современные оптоволоконные кабели отличаются высокой надежностью и длительным сроком службы без технического обслуживания в эксплуатации.
4. Все технические средства наложенных систем (безопасности, управления, передачи данных, телефонии, распределения телевизионных программ) подключаются к МСТС с помощью стандартного однотипного интерфейса Ethernet.
5. Для МСТС и всех наложенных систем возможно дистанционное централизованное управление из любой заданной проектом точки подключения.
6. МСТС обеспечивает возможность реконфигурации и развития подключенных и наложенных систем в течение длительного (многолетнего) срока эксплуатации без замены оборудования центрального и магистральных узлов.
7. Применение МСТС является решением опережающего технического уровня и тем самым наилучшим образом обеспечивает защиту капиталовложений заказчика в техническую инфраструктуру.

Приложение 2

Обеспечение информационной безопасности МСТС

На основе этого документа может быть разработано техническое задание для оснащения МСТС объекта (совокупности объектов) подсистемой информационной безопасности (ПИБ). Конфигурация описываемой ПИБ ориентирована на развертывание территориально распределенной МСТС, обслуживающей ИСБ нескольких разнородных объектов.

1. Технические требования по информационной защите СПВ ОВТ

К совокупности технических средств МСТС требования по защите информации предъявляются как к автоматизированной системе, построенной на базе средств вычислительной техники.

МСТС, стыкуемая с сетями связи общего пользования, должна быть защищена по классу защиты не ниже 1Г, в соответствии с требованиями РД ГТК «Автоматизированные системы. Защита от несанкционированного доступа к информации», а также «СТР-К». Подсистема информационной безопасности (ПИБ) МСТС/ИСБ должна представлять собой интегрированный комплекс программно-технических, технологических и организационных решений.

ПИБ МСТС/ИСБ должна создаваться с использованием модульных компонентов, построенных на базе архитектуры клиент/сервер, с организацией информационного обмена по стандартным сетевым протоколам (TCP/IP). Структура ПИБ МСТС/ИСБ должна обеспечивать возможность автономной работы при отказах отдельных компонентов программно-аппаратного обеспечения системы или каналов связи, обеспечивающих информационное взаимодействие и интеграцию модулей ПИБ МСТС/ИСБ.

В качестве аппаратных платформ ПИБ МСТС/ИСБ необходимо использовать средства с повышенной надежностью. Аппаратно-программные компоненты системы должны удовлетворять условию круглосуточной работы, позволять осуществлять резервирование и восстановление системы после сбоев.

В состав ПИБ МСТС/ИСБ включаются:

- подсистема управления доступом,
- подсистема регистрации и учета,
- криптографическая подсистема,
- подсистема обеспечения целостности.

2. Требования к подсистемам ПИБ

Общие требования к подсистемам управления доступом, регистрации, учета и контроля целостности (1Г).

Все пользователи и администраторы, допущенные к средствам МСТС/ИСБ, должны проходить строгую аутентификацию с использованием аппаратных средств хранения ключевой информации перед началом сеанса работы в системе.

Систему аутентификации наиболее целесообразно строить на аппаратной базе смарт-карт. Смарт-карты должны иметь техническую возможность совмещения в одном устройстве (карте) с картами доступа, используемыми для разграничения доступа в помещения защищаемых объектов. Используемые средства защиты от несанкционированного доступа должны иметь сертификат ФСТЭК (или Государственной технической комиссии при Президенте Российской Федерации).

Аутентификацию пользователей МСТС/ИСБ следует производить с использованием сертификатов открытых ключей (СОК), издаваемых в Удостоверяющем центре (УЦ). Для защиты от НСД и контроля целостности должны использоваться программно-аппаратные комплексы средств защиты информации от несанкционированного доступа (электронные замки).

Программно-аппаратные комплексы средств защиты информации от НСД должны обеспечивать:

- регистрацию пользователей компьютера и назначение им персональных электронных идентификаторов и паролей на вход в систему;
- запрос персонального электронного идентификатора и пароля пользователя при загрузке;
- возможность блокирования входа в систему при превышении предельного числа неудачных попыток входа, блокировании администратором входа пользователя;
- контроль целостности файлов на жестком диске;
- аппаратную защиту от несанкционированной загрузки операционной системы.

Электронные замки должны проверять персональный идентификатор и пароль пользователя при попытке входа в систему. В случае попытки входа в систему незарегистрированного пользователя электронный замок должен регистрировать попытку НСД. Загрузка операционной системы с жесткого диска любого должна осуществляться только после предъявления зарегистрированного электронного идентификатора.

Электронный замок должен осуществлять ведение системного журнала, записи которого хранятся в специальной энергонезависимой памяти. Электронный замок должен фиксировать в системном журнале вход пользователей, попытки входа, попытки НСД и другие события, связанные с безопасностью системы.

СЗИ от НСД при своем старте, а также периодически и по запросу администратора должна производить контроль целостности компонент прикладного программного обеспечения.

Требования к элементам, обеспечивающим функционирование ПИБ МСТС/ИСБ

Работа подсистем ПИБ, на уровне, обеспечивающем выполнение требований по безопасности, реализуется установкой и функционированием в составе ПИБ нескольких обеспечивающих подсистем. Важнейшие из них описаны ниже.

Требования к удостоверяющим центрам

Основной задачей УЦ, используемых в составе ПИБ, является поддержка функции установления криптозащищенных соединений между элементами МСТС/ИСБ. УЦ должны обеспечить:

- Издание сертификатов открытых ключей (СОК) с использованием сертифицированных ФАПСИ СКЗИ для субъектов и объектов доступа МСТС/ИСБ.
- Обеспечивать жизненный цикл СОК всех категорий пользователей (приостановку действия, отзыв, распространение информации о статусе и т.д.).
- Формирование и публикацию списков отозванных СОК с указанием даты и времени отзыва сертификатов в службе каталога.
- Возможность проверки статуса СОК в соответствии с использованием службы каталога.
- Ведение базы данных обо всех выпущенных сертификатах открытых ключей, ее резервное копирование и архивирование.
- Разделение функций Центра регистрации (ЦР) и Центра сертификации (ЦС).
- Двустороннюю аутентификацию соединений ЦС и ЦР.
- Формирование и выдачу СОК на бумажных носителях.
- Осуществление проверки подлинности ЭЦП документов в отношении выданных им СОК.
- Предоставление других, предусмотренных политиками УЦ, услуг участникам информационных систем в части, относящейся к его функциям.
- Ведение журналов работы УЦ.
- Простановку меток времени для операций с СОК.
- Возможность издания СОК с использованием алгоритмов ГОСТ Р 34.10-94, Р34.10-2001 и Р34.11-94.

Подсистема межсетевого экранирования

Для предотвращения возникающих угроз безопасности ИС при межсетевом взаимодействии по линиям связи сторонних операторов необходимо применять специальные программно-аппаратные

средства межсетевого экранирования. Подсистема МЭ должна:

- обеспечить разграничение доступа пользователей к ресурсам ИС на основе заданных правил;
- контролировать входящие/исходящие информационные потоки на нескольких уровнях модели информационного обмена OSI/ISO;
- проводить идентификацию и аутентификацию пользователей с защитой от прослушивания сетевого трафика;
- осуществлять трансляцию сетевых адресов и сокрытие структуры защищаемой сети от внешних субъектов;
- осуществлять управление информационными потоками и обеспечивать доступность сетевых сервисов;
- проводить антивирусную проверку входящих/исходящих информационных потоков;
- регистрировать запросы на доступ к ресурсам и результаты их выполнения;
- осуществлять автоматическое реагирование и сигнализацию попыток нарушения политики информационной безопасности;
- осуществлять централизованное управление политикой безопасности ИС.
- Иметь сертификат ФСТЭК (Гостехкомиссии России) на соответствие не ниже 3 класса защищенности.

Подсистема шифрования каналов связи (виртуальной частной сети, VPN)

Для защиты конфиденциальной информации, передаваемой по открытым каналам связи вне контролируемой зоны, необходимо применять криптографические средства построения виртуальных защищенных сетей. Средства VPN должны обеспечить:

- создание единого контура безопасности, объединяющего всех абонентов VPN – как сетей стационарных и подвижных объектов ВТ, а также отдельных пользователей;
- прозрачное кодирование межсетевых потоков;
- защиту соединений с мобильными пользователями и отдельными удаленными РС;
- выборочное кодирование трафика по IP-адресам;
- динамическое распределение и смену ключей кодирования;
- высокую производительность, достаточную для шифрования канала 100 Мбит/с;
- требуемое качество сервиса и поддержку работы с сервисами, предъявляющими высокие требования к величинам временных задержек (IP-телефония, видеоконференцсвязь);
- мониторинг и регистрацию событий безопасности;
- централизованное администрирование всех компонентов по защищенному каналу.

VPN-шлюзы каналов связи должны совмещаться с межсетевыми экранами соответствующих узлов МСТС на единой аппаратной платформе.

Подсистема обнаружения сетевых атак

Подсистема обнаружения атак должна предусматривать возможность прогнозирования и отражения атак в реальном масштабе времени, а также настраиваться на основе политики, обеспечивающей повышение уровня информационной безопасности в соответствии с появлением новых источников и средств реализации угроз.

Подсистема обнаружения атак должна обеспечивать возможность выполнения следующих основных функций:

- выявление информационных атак на прикладном уровне стека протоколов TCP/IP посредством анализа пакетов данных, передаваемых в СВУЦ;
- блокирование пакетов данных, нарушающих заданную политику безопасности;
- мониторинг трафика, циркулирующего на сетевом, транспортном и прикладном уровнях модели взаимодействия открытых систем;
- корреляция данных об информационных атаках с данными средств анализа защищенности (САЗ);
- обеспечение единого централизованного управления сетевыми датчиками обнаружения вторжений и средств анализа защищенности;
- оповещение администратора об обнаруженных атаках.

Подсистема обнаружения атак состоит из программных модулей реализующих функции датчиков обнаружения атак и менеджеров процессов. Подсистема обнаружения атак должна включать в себя два типа датчиков – сетевые и серверные. Сетевые датчики предназначены для перехвата и анализа всего сетевого трафика, передаваемого в рамках того сегмента, где установлен датчик. Серверные датчики предназначены для сбора и анализа информации только о тех пакетах данных, которые поступают на серверы с установленными датчиками. Серверные датчики должны обеспечивать возможность блокирования пакетов данных, представляющих угрозу безопасности информационным ресурсам МСТС/ИСБ. Сенсоры сетевого уровня должны иметь возможность анализировать трафик в реальном масштабе времени. Сенсоры хостового уровня должны иметь возможность анализировать как входящий трафик, так и журналы

операционной системы и приложений. Сенсоры хостового уровня должны поддерживать все виды ОС, используемых в МСТС/ИСБ. Все сенсоры должны управляться с помощью менеджера централизованного выделенного сервера. Все сенсоры должны иметь возможность автоматического централизованного обновления сигнатур атак. Сенсоры должны иметь возможность создания собственных правил, для описания трафика, который должен быть пропущен либо блокирован, или событий. Программное обеспечение сенсоров сетевого уровня должно иметь техническую возможность установки на ту же аппаратную платформу, что и МЭ.

Требования к подсистеме антивирусной зашиты
Подсистема антивирусной защиты МСТС/ИСБ должна быть централизованной. Средства антивирусной защиты должны быть сертифицированы на соответствие техническим условиям и требованиям РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия, не декларированных возможностей». Средства антивирусной защиты должны обеспечивать:

- защиту серверов и рабочих станций пользователей и администраторов, работающих под управлением ОС, используемых в МСТС/ИСБ;
- защиту почтовых систем;
- защиту шлюзов входа/выхода во внешнюю сеть.

Средства антивирусной защиты должны выполнять:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;
- проверку почтовых сообщений и вложений;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- возможность автоматического запуска сразу после загрузки операционной системы;
- автоматическую проверку съемных носителей информации.

Заключение

1. МСТС и работающая на ее технической базе ИСБ представляют собой автоматизированную систему (АС) со сложным алгоритмом функционирования, построенную на базе оборудования сходного по конструкции со средствами вычислительной техники (СВТ).
2. Существенная часть функциональных операций, в том числе все интеллектуальные действия ИСБ, выполняется на платформе СВТ.
3. Правильная и надежная работа СВТ, входящих в состав ИСБ и МСТС, является критически важной для безопасности защищаемого объекта.
4. Во многих случаях соображения экономической или технической целесообразности требуют стыковки и обмена данными между МСТС объектов контроля и сетью связи общего пользования.
5. По причинам, приведенным выше, МСТС и подключаемые к ней элементы ИСБ должны быть защищены от угроз, реализующихся через подключения к сети общего пользования на уровне, обеспечивающем их надежное функционирование.
6. Вследствие построения МСТС/ИСБ с использованием стандартизованных СВТ и приемов организации связи между ними (телекоммуникационных протоколов) обеспечение информационной безопасности системы ИСБ — МСТС должно строиться на основе стандартов по безопасности автоматизированных систем и реализовываться разработанными и аттестованными для этой цели средствами.
7. Надежность и уровень защиты информации в системе ИСБ — МСТС оценивается с использованием критериев, применяемых для АС общего назначения, построенных на базе СВТ.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Лапина И.К. *(lapina@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати **32555**