Личная безопасность гостей, работников гостиницы и их собственности

Концепция системы безопасности гостиницы

Понятие безопасности включает в себя не только защиту от криминальных посягательств, но еще в большей степени создание предупредительных мер обеспечения защиты от пожара, взрыва и других чрезвычайных происшествий.

Эффективное решение этой проблемы требует системного подхода, основанного на анализе функционирования объекта, выявления наиболее уязвимых зон и особо опасных угроз, составления всех возможных сценариев криминальных действий и выработке адекватных мер противодействия.
Комплексный подход предусматривает оптимальное сочетание организационных, технических и физических мер предупреждения и своевременного реагирования на любую опасную ситуацию. Ключевое значение приобретает правильный выбор технических средств и систем безопасности, их правильное проектирование, монтаж и обслуживание.
Основными причинами, выводящими применение технических средств на главенствующие позиции среди мер обеспечения безопасности, являются:

- неподверженность (в отличие от людей) усталости, невнимательности, болезням, сиюминутным чувствам, погодным условиям;
- неподкупность, невозможность обмана, шантажа и запугивания;
- мгновенность реакции, точность выполнения заложенных функций.

В современных условиях преступный мир проявляет интерес не только к банкам, хранилищам ценностей, складам, но не оставляет без внимания и гостиницы как мелкие, так, в особенности, высококлассные гостиничные комплексы, Только создание эффективной, надежной и всесторонней системы безопасности позволит гостинице иметь имидж мирного доброжелательного дома, гарантирующего всем гостям спокойствие и уверенность в своей безопасности.

Гостиницы, как объекты внедрения комплексных систем безопасности, имеют некоторые принципиальные отличия от промышленных или военных (режимных) объектов. Основными из них являются:

- гостиница заинтересована в создании имиджа открытого дома с обеспечением режима наибольшего благоприятствования для максимального числа гостей, поэтому любые устройства безопасности не должны иметь устрашающего вида, но в то же время внушать гостю чувство личной безопасности и комфортности;
- гостиницы, как правило, находятся в городской черте, в среде активного движения транспорта и пешеходов;
- система прохода в гостиницу и в номера должна быть предельно простой и не создавать для гостя больших затруднений.

КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СОВРЕМЕННОЙ ГОСТИНИЦЫ

Основные цели:

- ПОВЫШЕНИЕ ПОЖАРНОЙ И АВАРИЙНОЙ БЕЗОПАСНОСТИ ГОСТИНИЦ;
- ЗАЩИТА ГОСТЕЙ,ПЕРСОНАЛА И ИМУЩЕСТВА ОТ КРИМИНАЛЬНЫХ ПОСЯГАТЕЛЬСТВ;
- СОВЕРШЕНСТВОВАНИЕ ТЕХНОЛОГИИ ГОСТИНИЧНОГО ОБСЛУЖИВАНИЯ.

Все это достигается путем осуществления комплекса взаимосвязанных мер по обеспечению безопасности, отвечающего современным международным стандартам, включая оснащение гостиничных зданий новейшими техническими средствами, проведение тактико-организационных мероприятий.

Анализ возможных угроз

- пожар, причиной которого может быть небрежность гостей, неисправность электрооборудования, несоблюдение или нарушение правил противопожарной безопасности обслуживающим персоналом, умышленный поджог;
- взрыв, вызванный проносом и установкой взрывчатки в криминальных целях, или взрыв газа при его утечке (особенно вероятно в местах приготовления пищи в ресторанах, барах при использовании газового оборудования);
- несанкционированный проход посторонних лиц в номера при отсутствии гостей с целью кражи ценностей, документов, установки взрывных устройств или подслушивающей аппаратуры;
- несанкционированный проход в номера обсуживающего персонала с теми же криминальными целями, обусловленный криминальными мотивами или шантажом преступников;
- нападение на гостя в номере, лифте или в другом месте гостиницы;
- нападение на кассу в рабочее время или попытка ее вскрытия в нерабочее время;
- нападение на администрацию гостиницы с целью шантажа, требования открыть кассу или нейтрализовать систему безопасности;
- террористический акт со взятием заложников клиентов гостиницы или попытка подрыва или поджога;
- вооруженное нападение на номера, арендуемые у гостиниц коммерческими фирмами под офисы.

Тактико-организационные меры

Традиционный метод усиления безопасности путем увеличения численности сотрудников не дает желаемого результата как из-за экономических соображений, так и малой эффективности такого подхода. Человек, несущий службу, подвержен утомляемости, невнимательности, не исключен сговор с преступниками, шантаж, запугивание и т. д.. Единственное, правильное решение вопроса безопасности *использование системного, комплексного подхода, сочетающего в себе методы организационного, технического и физического характера* в их правильном сочетании и разумном определении доли каждой составляющей.

К организационным мерам относятся:

- специально разработанные системы регламентации поведения обслуживающего персонала и сотрудников, отвечающих за безопасность;
- проведение мер по специальной подготовке персонала службы безопасности;
- технология гостиничного обслуживания;
- принципы организации порядка доступа и охраны различных категорий гостиничных номеров и служебных помещений;
- регламентация действий сотрудников в экстремальных ситуациях.

Очевидно, что переход к новой, современной концепции безопасности, предусматривающей применение сложной специальной техники, требует пересмотра тактических аспектов в работе различных служб гостиницы.

Необходимо реализовать следующие организационные меры:

- разработать детальные инструкции по действиям во всех возможных нештатных ситуациях и довести их до каждого сотрудника;
- составить краткие, красочные, высокоинформативные и интуитивно понятные инструкции по пользованию аппаратурой безопасности для гостей, в которые должны быть внесены краткие правила поведения в экстремальной ситуации;
- регулярно проводить занятия по повышению квалификации персонала службы безопасности, физической и боевой подготовке;
- провести обучение всего персонала гостиницы правилам пользования аппаратурой комплекса безопасности;
- организовать для персонала периодическую(не менее одного раза в год)проверку знаний в области безопасности, проводить дополнительное обучение по мере смены кадров и модернизации комплекса;
- организовать немногочисленную, но профессиональную инженерную службу (в рамках штата службы безопасности). В обязанности которой вошло бы проведение технического обслуживания комплекса автоматизации здания, проведение обучения и консультирования сотрудников прочих служб гостиницы;
- прочие меры (разрабатываются индивидуально для каждого конкретного гостиничного комплекса).

приоритетные направления обеспечения безопасности современной гостиницы:

- **контроль доступа на объект;**
- **комплекс мер по противопожарной защите;**
- **охранная сигнализация и видеонаблюдение.**

Основные подсистемы комплекса технических средств безопасности:

Система пожарной безопасности:

система пожарной сигнализации, датчики; система визуально звукового оповещения; система пожаротушения;

система вентиляции и дымоудаления;

система разблокировки выходов(интеллектуальная!)

Система охранной сигнализации эффективное и своевременное обнаружение факта несанкционированого проникновения в охраняемые помещения (площадки, зоны) с точным определением места, оповещение сотрудников службы безопасности, милиции (вневедомственной охраны), документирование информации.)

Защите с помощью средств охранной сигнализации подлежат:

- внешний периметр гостиничного комплекса,
- парковки автотранспорта,
- внешний контур гостиницы,
- ответственные служебные помещения, такие как касса, камера временного хранения ценностей, кладовые, кабинеты администрации гостиницы, разного рода аппаратные и пультовые,
- гостиничные номера,
- прочие площадки, зоны, помещения.

для обнаружения факта несанкционированного проникновения используются различные типы сигнализационных датчиков. Вследствие огромного разнообразия существующих типов датчиков, кратко упомянем лишь наиболее распространенные типы, сгруппировав их по классам защищаемых объектов:

- датчики, устанавливаемые на внешних ограждениях (емкостные, радиолучевые, проводноволновые, активные инфракрасные, вибрационные и др.) используются для охраны периметра (внешней границы) гостиничного комплекса и парковок автотранспорта;
- датчики, охраняющие открытые площадки (микроволновые, инфракрасные пассивные, комбинированные) применяются для охраны парковок автомобилей;
- датчики, сигнализирующие об открывании или разрушении дверей, окон (магнитоконтактные, вибрационные, инфракрасные активные и пассивные) применяются для охраны дверей здания, в том числе лифтов, предоставляют информацию для системы управления доступом;
- датчики, реагирующие на разбитие стекла (акустические, вибрационные);
- датчики, блокирующие внутренние объемы помещений (инфракрасные пассивные, микроволновые, ультразвуковые, комбинированные, барометрические и др.;
- датчики, охраняющие отдельные предметы (емкостные, вибрационные и др.), используемые для охраны отдельных, особо ценных объектов сейфов, витрин с ценностями, шкафов с оружием и т.д.

Информация от охранных датчиков собирается центральной станцией охранной сигнализации (системой сбора и обработки информации), выполняющей функции контроля состояния и работоспособности датчиков, шлейфов, исполнительных устройств, передачи информации, документирования. Функции центральной станции могут выполнять:

- специализированный приемно контрольный прибор или многофункциональный приемноконтрольный прибор систем пожарной, охранной и тревожновызывной сигнализации (при автономной или полуавтономной организации системы безопасности);
- модули (концентрирования информации, отображения, интерфейса, исполнительные и др.)интегрированной системы безопасности.

Учитывая большое количество точек охраны, сложный и непредсказуемый режим функционирования объекта, необходимость соблюдения принципа максимизации показателя эффективность/стоимость и наличие мощных систем ограничения доступа и телевизионного наблюдения, достаточным может быть сочтен принцип минимального оснащения гостиничных номеров сигнализационными средствами. По тем же причинам необходима реализация децентрализованного принципа охраны, т.е. постановка и снятие с охраны производит сам клиент.
Естественно, это не относится к некоторым другим помещениям повышенной важности, таким как сейфовая, касса, кладовые и т. п. При оснащении этих помещений должен использоваться принцип многорубежности, т.е. применения нескольких концентрических колец сигнализации, окружающих охраняемый объект.

Система тревожно вызывной сигнализации (срочный вызов (оповещение о возникновении тревожной ситуации) службы безопасности. В приложении к данной задаче система тревожно вызывной сигнализации может также использоваться для подачи различного рода сигналов клиентом гостиницы горничным, техникам и т. д.)

Для подачи сигнала могут быть использованы различного рода устройства:

- механические тревожные кнопки могут быть ручными, ножными, скрытыми;
- носимые радиокнопки (радиобрелки) могут быть одно и многокнопочными (для подачи различного рода сигналов), совмещенными с пользовательской пластиковой карточкой системы доступа, позволяющими идентифицировать личность подавшего сигнал, его точное местоположение и т. п.
- сигнал тревоги или вызова может быть также подан с других устройств, принадлежащих другим системам выносных пользовательских пультов станции охранной сигнализации, кодонаборных панелей системы управления доступом, путем набора особого "кода тихой тревоги" *когда клиента или сотрудника вынуждают отключить или вскрыть ту или иную систему под угрозой оружия, он может набрать особый код и тогда система действительно отключится, но при этом на пост службы безопасности поступит тревожное сообщение о том, что отключение произошло под принуждением.*

Система управления доступом (обеспечение беспрепятствованного саннкционированного доступа в помещения и блокирование несанкционированного доступа. Организация режима доступа (по временному расписанию, по иерархии, в зависимости от оплаченных клиентом услуг и т. п. Учет рабочего времени сотрудников. Документирование информации.)

Наиболее распространенным в современной гостиничной практике является использование автономных замков с пластиковой карточкой системы VingCard
Преимущества: относительная дешевизна, простота использования для клиента, надежность.
Недостатки: отсутствие возможности централизованного получения информации в режиме online, сложности при необходимости перепрограммировать замок или считать накопившийся протокол событий (осуществляется последовательный обход замков с переносным компьютером Note Book), кроме того, выигрыш в прокладке кабельных линий относителен все равно необходим подвод линий для подачи сигнала экстренного разблокирования.
Более перспективной (хотя и более дорогостоящей) на сегодняшний день представляется **идея создания сетевой (online) системы с централизованным контролем.** Такая система позволит оператору службы безопасности (а также менеджеру отеля, представителям других служб) постоянно держать контроль над ситуацией на объекте, знать, какие помещения открыты, закрыты, разрешать или запрещать доступ и т. п., можно даже разрешить или запретить определенным лицам останавливать лифт на

Индивидуальные пластиковые карточки : используются в качестве "электронного ключа", обеспечивая доступ в помещения по определенному алгоритму.
Существуют следующие основные типы карт:

- перфорированные наиболее дешевые, перезапись невозможна;
- магнитные наиболее распространенные, низкая стоимость;
- штрихкодовые надежные, низкая стоимость, без перезаписи;
- viegand (индуктивные) перезапись невозможна, средняя стоимость;
- proximiti с дистанционным считыванием, относительно дорогие;
- smart (со встроенным чипом) наибольшее количество функций, практически невозможно подделать, самые дорогие;
- комбинированные
- Считыватели пластиковых карт: для считывания информации с карт.
- Кодонаборные устройства: для набора индивидуального кода; иногда совмещаются со считывателем карт, в этом случае код служит для подтверждения факта санкционированного использования карты.
- Контроллеры считывающих устройств: обрабатывают информацию, поступающую от считывателей и кодонаборников и передают ее на центральную станцию (главный контроллер), разрешают или запрещают доступ в соответствии с заложенным алгоритмом, управляют замками.
- Центральная станция системы управления доступом: как правило персональный компьютер, сервер, иногда главный контроллер или и то, и другое. В интегрированных комплексах безопасности соответствующие модули или непосредственно сервер комплекса. Используется для контроля, обработки, отображения и документирования поступающей информации, управления режимом доступа, программирования локальных контроллеров, организации взаимодействия с другими системами комплекса безопасности, приема передачи информации.
- Оборудование для изготовления карт, записывания определенной информации.
- Замковые дверные устройства: электромеханические и электромагнитные замки, электрозащелки, дверные доводчики и т. д.
- Прочие устройства, включая тамбуры, шлюзы, проходные кабины, детекторы металлов. Для условий гостиницы эти устройства могут применяться с большими ограничениями.

С точки зрения экономии средств в качестве индивидуальных карт наиболее целесообразно использовать обычные пластиковые карты с магнитной кодировкой. Для клиентов класса VIP могут быть рекомендованы proximiti карты (считываются дистанционно, даже находясь внутри бумажника в нагрудном кармане). Карта выдается клиенту при регистрации. Система настраивается таким образом, что доступ клиенту в номер разрешен ровно на оплаченный срок пребывания в гостинице. Кроме того, возможно разрешение/запрет на доступ в те или иные помещения (зоны, этажи) в зависимости от оплаченного комплекса услуг, класса и т.п. Приходящим гостям, посетителям, не являющимся клиентами гостиницы, могут также выдаваться индивидуальные карты, разрешающие, например, только доступ на определенный этаж в течение определенного времени.

Возможны самые разнообразные настройки системы для ее реакции в случае попытки несанкционированного прохода. Например, если зафиксирована попытка воспользоваться гостевой картой в рамках разрешенного маршрута, но вне заданного времени, система может или просто запретить проход, или разрешить его, немедленно оповестив службу безопасности.

Обслуживающий персонал гостиницы, сотрудники службы безопасности имеют персональные карты, разрешающие доступ в определенные (или во все номера). При каждом факте входа в номер центральная станция фиксирует, кто и когда вошел.

Обычно, для большей эффективности системы контроля доступа на особо важных объектах (банки, фабрики драгметаллов и т. д.) применяются шлюзовые или тамбурные проходные кабины, которые практически исключают любую возможность несанкционированного прохода и блокируют нарушителя в замкнутом объеме кабины. Однако применение подобных устройств в гостиницах вряд ли целесообразно, так как создает массу неудобств для клиентов и их гостей. Хотя для отдельных помещений (касса, хранилище ценностей) оно может быть рекомендовано. Аналогично, может быть рекомендовано локальное применение средств обнаружения металлов (оружия), взрывчатых веществ. Например, стационарные детекторы арочного типа могут быть установлены на входе в зоны или отдельные номера категории люкс, а уже пользоваться ими или нет решает хозяин номера или его личная охрана. Рекомендуется оснастить службу безопасности переносными обнаружителями оружия и взрывчатки.

Система телевизионного наблюдения (обеспечение визуального контроля за обстановкой на объекте, анализ нештатных ситуаций, верификация (проверка истинности)поступающих сигналов тревоги, помощь в принятии оперативных решений, протоколирование визуальной информации.)

Такие системы включают, как правило, от нескольких десятков до сотен телевизионных камер, несколько постов наблюдения, оснащенных мониторами и вынесенными пультами управления

Построение: видеоинформация собирается телевизионными камерами (чернобелыми или цветными). Рекомендуются (применительно к оснащению гостиничного комплекса) следующие принципы установки камер:

- открыто (без маскировки): по периметру здания, на парковках автотранспорта, в зоне центрального входа, зале регистрации, в крупных холлах, помещениях особой важности, в служебных помещениях;
- скрыто (маскировка в часы, светильники, предметы интерьера, замуровывание в стену) в зонах расположения гостиничных номеров, в помещениях особой важности (дублируются открыто установленные камеры).

Вообще, при выборе типа установки нужно учитывать следующее обстоятельство: *открыто установленная камера, с одной стороны, "отпугивает" потенциального преступника, с другой стороны, создает определенный моральный дискомфорт для клиентов.*

Видеоинформация от камер поступает в центральную пультовую, где с помощью разного рода видеокоммутационных устройств осуществляется обработка видеосигналов (наложение даты, времени, имени или номера камеры, совмещение изображений и т. д.), вывод видеоинформации на мониторы, запись на видеорегистрирующие устройства, распределение информации между постами (пультовыми), взаимодействие с прочими системами комплекса безопасности.

наиболее употребимые, относительно данной задачи, приборы и устройства, применяемые для организации системы телевизионного наблюдения:

- матричный коммутатор: "сердце системы; осуществляет сбор информации от всех камер, осуществляет ее распределение между всеми устройствами системы, прочими постами охраны, пультовыми других служб гостиницы (причем выводится только та информация, которая попадает в сферу компетенции соответствующего поста/службы;
- устройства отображения мониторы;
- устройства совмещения изображения (в том числе квадраторы):позволяют просматривать на экране одного монитора изображения от нескольких камер одновременно;
- генераторы даты/времени: позволяют "накладывать № на видеосигнал текстовую информацию, текущую дату и время;
- детекторы движения: формируют сигнал"тревога" при изменении обстановки в поле зрения камеры (например, при проходе человека или загорании);
- видеомультиплексоры: позволяют производить запись на один видеомагнитофон информации от нескольких (до 16) камер одновременно; при применении этих устройств может быть организована круглосуточная запись от всех камер ;
- видеоусилители: позволяют увеличивать допустимую длину кабельной линии между камерой и центральной пультовой;
- прочие устройства, включая устройства наведения, соответствующие контроллеры, системы передачи видеоинформации по телефонным линиям и т. д.

Система защиты информации

Защите подлежит следующая информация:

- *Информация о клиентах категории VIP*
- *Информация, обсуждаемая или обрабатываемая с применением технических средств во время совещаний в специально выделенных помещениях.*
- *Коммерческая тайна.*
  Защита сведений, осуществляется посредством определенных организационно технических мероприятий. К организационным мерам следует отнести ограничение доступа к защищаемым сведениям и введение административной и правовой ответственности за их разглашение. Технические меры имеют целью исключить утечку защищаемых сведений по техническим каналам:
- за счет прослушивания по акустическим и виброакустическим каналам
- за счет побочных электромагнитных излучений и наводок технических средств связи, электропитания , радиотелевизионной приемной аппаратуры, электробытовых приборов, оргтехники и т.д.;
- по оптическому каналу;
- за счет средств несанкционированного съема информации (закладок).

Технические меры защиты включают в себя:

- применение проектных решений, обеспечивающих требуемую звукоизоляцию ограждающих конструкций стен, полов потолков:
- оснащение окон защищаемых помещений защитными жалюзи, шторами, пленкой;
- использование сертифицированных средств технической защиты от побочных радиоизлучений
- периодическую проверку защищаемых помещений и установленных в них средств на отсутствие закладок.
- Реализованные меры защиты от утечки информации отражаются в аттестате помещения, который при необходимости выдается клиентам категории VIP, а также представителям организаций, ответственным за проведение конфиденциальных мероприятий в специально выделенных помещениях.

Противоаврийный контроль систем жизнеобеспечения здания (газ, вода, электричество)(контроль и блокирование в случае аварии (пожара, стихийного бедствия, угрозы терракта) систем жизнеобеспечения гостиничного комплекса.)

Функции контроля и блокировки систем жизнеобеспечения здания являются стандартными для крупных интегрированных комплексов (пример: системы Honeywell), что выводит их в разряд систем полной автоматизации здания. Кроме указанных функций контроля и блокировки, такие комплексы "умеют" управлять освещением, лифтами, терморегуляцией (отопление, вентиляция) и т.д.

Система электропитания слаботочных устройств

Основные требования к системе электропитания комплекса технических средств безопасности:

- питание всех подсистем и приборов должно раздаваться централизовано (все блоки питания в центральной пультовой аппаратной; такая система гарантирует повышенную техническую надежность, а также защиту от саботажа и упрощает техническое обслуживание.
- магистральное электропитание комплекса от сети 220 вольт должно выполняться по первой категории (от двух независимых фидеров);
- для наиболее важных компонентов комплекса (главный сервер, компьютеры систем безопасности, основные контроллеры) должно предусматриваться резервное питание от аккумуляторов в течении, по меньшей мере, двух часов.

Система оперативной связи(обеспечение оперативной связи между пультовыми и постами службы безопасности, отдельными сотрудниками службы безопасности и прочими службами.)
Построение: все пультовые, посты охраны и наблюдения оснащаются многоканальными переговорными устройствами (желательно с трубками телефонного типа из соображений конфиденциальности), сотрудники службы безопасности, инженерных служб обеспечиваются носимыми радиостанциями

Техническая укрепленность здания гостиницы(создание физических барьеров, препятствующих несанкционированному проникновению в здания гостиничного комплекса, путем разрушения (взлома) инженерных конструкций здания.)
Построение: данная задача в максимальной степени может быть решена только при строительстве нового здания или при генеральной реконструкции, допускающей перепланировку. В прочих случаях могут быть рекомендованы следующие меры повышения технической укрепленности здания:

- установка металлических решеток на окнах первого и цокольного этажей, оклейка стекол указанных окон, а также окон гостиничных номеров (всех или только категории люкс) защитной пленкой;
- установка металлических дверей на входах в наиболее ответственные помещения и блоки помещений;
- оснащение наиболее важных дверей высококачественными замковыми устройствами,
- установка турникетов, проходных кабин, шлюзов.

Создание комплексной интегрированной системы безопасности позволяет не только значительно повысить степень обеспечения безопасности здания и его обитателей, но и значительно повысить качество обслуживания клиентов, облегчить работу обслуживающего персонала и т.д.

Спасибо за внимание!!!