**Система безопасности гостиничного комплекса**

2012

Диплом

Интенсивное развитие индустрии туризма и гостеприимства, как в нашей стране, так и в мире в последние годы проходит на фоне усиления международного терроризма, локальных военных конфликтов, ухудшения криминальной обстановки.

Введение

Интенсивное развитие индустрии туризма и гостеприимства, как в нашей стране, так и в мире в последние годы проходит на фоне усиления международного терроризма, локальных военных конфликтов, ухудшения криминальной обстановки.

Гостиница является местом отдыха и, как следствие, повышенного скопления людей. Безопасность гостей, персонала, а также защита информации, одна из важнейших проблем, которую должно решить руководство отеля. Администрация гостиницы берет на себя обязательства, не только обеспечить уют проживания и гарантии хорошего отдыха, но и безопасность людей, проживающих в гостиницах, их жизни, здоровья, имущества и т.д. Поэтому, необходим тщательнейший контроль по обеспечению безопасности гостиницы.

**Вернуться в каталог готовых дипломов и магистерских диссертаций –**

[**http://учебники.информ2000.рф/diplom.shtml**](http://учебники.информ2000.рф/diplom.shtml)

Под безопасностью гостиницы понимается личная безопасность туристов, сохранность их имущества и не нанесении ущерба окружающей природной среде при совершении путешествий. Данная дефиниция из закона РФ «Об основах туристской деятельности» [5] не совсем точна. Безопасность не может быть абсолютной. В то же время уровнем опасности можно управлять (устанавливать санитарно-защитные зоны вокруг опасных объектов, уменьшать массу хранящихся опасных веществ и др.). Безопасность, это не только надежная защита от грабителей, пожаров, террористов, но это и защита гостей и персонала от казусов природы, защита от болезней, от техногенных катастроф. Также не надо забывать о том, что надо защитить техническую базу компьютеров, например, от проникновения хакеров, вирусов, утечки информации. Изменения в такой обширной области, как информационная безопасность, уже давно не ограничиваются только лишь совершенствованием программных и аппаратных средств защиты. Появляются новые виды угроз, меняются взгляды компаний на подходы к организации безопасности.

Любой гостинице и ее гостям угрожают кражи, ограбления, пожары, поджоги, массовые отравления, теракты, буйство гостей и халатность персонала, неисправности в работе различных систем и многое, многое другое. Поэтому любые меры, силы и средства, используемые для обеспечения безопасности гостиницы, не должны иметь устрашающего вида, но в то же время внушать постояльцу чувство личной безопасности и комфортности. О безопасности здесь заботятся двадцать четыре часа в сутки, и насколько эффективны современные методы зависит от квалифицированности персонала, технического обеспечения безопасности и т.п.

Таким образом, системы обеспечения безопасности и защита информации постепенно превращаются в комплексы, позволяющие контролировать многие параметры объектов и процессы, на них происходящие. [30]

В данной выпускной квалификационной работе мы рассматриваем тему обеспечения безопасности в гостинцах и предотвращение риска для жизни и здоровья постояльцев и работников. Этим и обоснована актуальность темы данной выпускной квалификационной работы.

Цель настоящей выпускной квалификационной работы — разработать оптимальную систему безопасности в гостинице.

Объектом исследования выступает безопасность в гостинице ООО «Новотель» «Калуга Плаза» города Калуга.

Предметом исследования является работа службы безопасности гостиницы ООО «Новотель» «Калуга Плаза»

Для достижения поставленной цели в работе поставлены следующие задачи:

·        рассмотреть основные аспекты безопасности в гостинице;

·        проанализировать существующие системы безопасности в гостинице «Калуга Плаза»;

·        разработать систему безопасности гостиничного комплекса.

Методы исследования, применяемые в работе: анализ отечественной и зарубежной литературы по проблеме исследования системы безопасности гостиничных предприятий; анализ результатов устного опроса клиентов гостиницы «Калуга Плаза» и мер, принятых руководством организации, по работе службы безопасности.

Структурно работа состоит из введения, трех глав, заключения и списка использованных источников.

Первая глава посвящена рассмотрению основ безопасности в туризме и гостиничном бизнесе.

Во второй главе проводится анализ системы безопасности гостиницы ООО «Новотель» «Калуга Плаза».

Третья глав посвящена разработке системы безопасности гостиничного комплекса.

Практическое значение данной выпускной квалификационной работы заключается в разработке системы безопасности гостиничного комплекса.

1. Теоретические основы безопасности в гостиничном бизнесе безопасность работник гостиница риск 1.1 Служба безопасности гостиничного комплекса (предприятия), правовые основы ее деятельности

Российское законодательство определяет безопасность как гарантированную законодательными и практическими мерами защищенность жизненно важных интересов от внутренних и внешних угроз.

Критерии безопасности объекта — это критерии, по которым оцениваются жизненно важные условия существования объекта. Основные положения, состав и организация службы безопасности имеют юридическую силу в том случае, если они соответствуют положениям, зафиксированным в основополагающих правовых документах.

Каждая фирма представляет собой систему, включающую основные элементы и связи между ними. Система — это совокупность объектов, взаимодействие которой обуславливает наличие интегративных качеств, не свойственных ее частям, компонентам. Как раз по линиям внутренних и внешних связей системы (фирмы) могут реализовать угрозы ее экономической безопасности.

В основу деятельности службы безопасности положены: Гражданский Кодекс РФ [1]; Федеральный Закон «О безопасности» [2]; Закон РФ «Об информации, информационных технологиях и о защите информации»[3]; Федеральный Закон «О коммерческой тайне»[6]; Инструкции министерств и ведомств, касающиеся соответствующих видов деятельности; Устав объекта (предприятия), коллективный договор, трудовые договоры, правила внутреннего трудового распорядка сотрудников, должностные обязанности руководителей и персонала объекта (предприятия).  
1.2 Теоретические аспекты безопасности в гостинице

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.

|  |
| --- |
| [Вернуться в библиотеку по экономике и праву: учебники, дипломы, диссертации](http://учебники.информ2000.рф/index.shtml)  [Рерайт текстов и уникализация 90 %](http://учебники.информ2000.рф/rerait-diplom.shtml)  [Написание по заказу контрольных, дипломов, диссертаций. . .](http://учебники.информ2000.рф/napisat-diplom.shtml) |

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 постоянного роста преступности и осложнения криминогенной обстановки вопрос обеспечения безопасности любого объекта выходит на одно из первых мест. 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 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 которых 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 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.

Создание комплекса безопасности гостиницы — один из тех случаев, когда система контроля доступа, охранно-пожарная сигнализация и система видеонаблюдения служат не только для охраны помещений, но и для контроля за постояльцами, посетителями и персоналом. Разумеется, и подходы к ее построению во многом отличаются от других объектов.

Опасности физического и социального характера должны приниматься в расчет субъектами индустрии туризма, которым следует минимизировать и предотвращать разнообразные угрозы безопасности туристской деятельности. Обеспечение безопасности предусматривает целый комплекс мероприятий в рамках национального законодательства, гарантирующих безопасность перемещения туристов и гостей зарубежных стран по территории государства, их пребывания, сохранность здоровья, жизни и имущества.

Федеральный закон [2] определяет основные принципы и содержание деятельности по обеспечению безопасности государства: общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации (далее — безопасность, национальная безопасность), полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации (далее — Совет Безопасности).

Рассмотрим основные положения данного Закона. Общие положения, определяющие суть и области приложения данного Закона, рассматриваются в разделе 1 «Общие положения», в который входят следующие статьи [2]:

·        ст.1. Предмет регулирования настоящего Федерального закона;

·        ст.2. Основные принципы обеспечения безопасности;

·        ст.3. Содержание деятельности по обеспечению безопасности;

·        ст.4. Государственная политика в области обеспечения безопасности;

·        ст.5. Правовая основа обеспечения безопасности;

·        ст.6. Координация деятельности по обеспечению безопасности;

·        ст.7. Международное сотрудничество в области обеспечения безопасности.

На их защиту и направлены рассматриваемые нами в дальнейшем законодательные акты.

К основным объектам безопасности относятся: соблюдение и защита прав и свобод человека и гражданина; законность; системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности; приоритет предупредительных мер в целях обеспечения безопасности; взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Государство обеспечивает правовую и социальную защиту гражданам, общественным и иным организациям и объединениям, оказывающим содействие в обеспечении безопасности в соответствии с законом.

Под угрозой безопасности понимается совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества, государства, реальную и потенциальную угрозу. Источники опасности внешние или внутренние определяют содержание деятельности по обеспечению внутренней и внешней безопасности.

Обеспечение безопасности достигается проведением единой государственной политики, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества, государства.

Обеспечение безопасности личности, общества и государства осуществляется на основе разграничения полномочий органов законодательной, исполнительной и судебной властей в данной сфере.

Вопрос обеспечения безопасности в туризме освещен в федеральном законе «Об основах, туристской деятельности в Российской Федерации»[5].

Основными целями государственного регулирования туристской деятельности являются:

·        обеспечение права граждан на отдых, свободу передвижения и иных прав при совершении путешествий;

·        охрана окружающей среды;

·        создание условий для деятельности, направленной на воспитание, образование и оздоровление туристов;

·        развитие туристской индустрии, обеспечивающей потребности граждан при совершении путешествий, создание новых рабочих мест, увеличение доходов государства и граждан Российской Федерации, развитие международных контактов, сохранение объектов туристского показа, рациональное использование природного и культурного наследия. Приоритетными направлениями государственного регулирования туристской деятельности являются поддержка и развитие внутреннего, въездного, социального и самодеятельного туризма.

В целях защиты прав и интересов туристов осуществляются лицензирование, стандартизация туроператорской и турагентской деятельности, а также объектов туристской индустрии, сертификация туристского продукта.

Гостиница относится к предприятиям, оказывающим туристические услуги населению и руководствуется ГОСТ Р 50644-2009 «Требования по обеспечению безопасности туристов и экскурсантов» [10]. Настоящий стандарт устанавливает требования по обеспечению безопасности жизни, здоровья, имущества туристов при совершении путешествий.

Настоящий стандарт распространяется на юридических лиц независимо от их организационно — правовой формы и формы собственности, индивидуальных предпринимателей, оказывающих туристические услуги.

Туристские услуги и условия их предоставления должны быть безопасными для жизни, здоровья и имущества туристов и окружающей среды.

В процессе оказания туристских услуг необходимо обеспечить приемлемый уровень риска для жизни, здоровья и имущества туристов (экскурсантов) при совершении путешествий.

Гостиничное предприятие, в соответствии со статьей 925 ГК РФ [1] отвечает за сохранность вещей потребителя, а также несет ответственность за вред причиненный жизни, здоровью и имуществу потребителя. Вследствие недостатков при оказании услуг, а также несет ответственность за вред, причиненный жизни, здоровью или имуществу потребителя вследствие недостатков при оказании услуг, а также компенсирует моральный вред, причиненный потребителю нарушением прав потребителя.

Специфика обеспечения безопасности в гостиничном бизнесе проста. Как правило, гостиница представляет собой отдельное многоэтажное строение с одним парадным входом и несколькими служебными. Кроме жилых номеров, в здании часто размещаются ресторан и бар, игровые залы и салоны красоты. Обычно несколько этажей отводятся для деловых целей: там размещаются администрация гостиницы, частные офисы, конференц-залы и залы для совещаний. На остальных этажах расположены жилые номера. Таким образом, основная сложность при разработке системы безопасности гостиницы связана с хаотичными перемещениями большого количества посетителей.[34]

При этом необходимо соблюдать главное условие. Принятый комплекс мер должен не только обеспечить клиентам гостиницы и ее сотрудникам защиту от возможных чрезвычайных происшествий, но и позволить им чувствовать себя уверенно, спокойно и комфортно.

Гостиницы, как объекты безопасности, имеют принципиальные отличия от промышленных или режимных объектов. Администрация крайне заинтересована в создании имиджа «открытого дома» с обеспечением режима наибольшего благоприятствования для максимального числа гостей, поэтому любые устройства безопасности не должны привлекать внимание посетителей, но, в то же время, обеспечивать чувство личной безопасности и комфортности.

Гостиницы, чаще всего, 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 гостей больших затруднений.

По отношению к гостиничному комплексу понятие безопасности включает в себя не только защиту от криминальных посягательств, но, еще в большей степени, создание предупредительных мер обеспечения защиты от пожара, аварийных ситуаций, необоснованного вмешательства в личную и деловую жизнь гостей, злоупотреблений персонала, других факторов дискомфорта. Кроме того, оптимальное решение в сфере безопасности должно способствовать совершенствованию технологии гостиничного обслуживания.

Работа персонала гостиницы предполагает индивидуальный подход к каждому посетителю. А в сфере безопасности ключевое значение приобретает правильный выбор технических средств, оптимальное проектирование систем, их монтаж и обслуживание.

Технические средства являются основой системы безопасности гостиницы по нескольким причинам. Во-первых, техника не подвержена усталости, невнимательности, болезням, сиюминутным чувствам, погодным условиям. Во-вторых, к ней неприменим подкуп, шантаж и запугивание, и неспециалисту сложно ее обмануть. Ну и, в-третьих, в ней изначально предусмотрены мгновенная реакция и точность выполнения заданных алгоритмов. Однако эти преимущества должны в обязательном порядке дополняться возможностями сотрудников службы безопасности. Только тесное взаимодействие специалистов и техники способно обеспечить оперативное реагирование на тревожную ситуацию и комплексно разрешить возникающие проблемы.

Среди приоритетных направлений обеспечения безопасности современной гостиницы следует назвать контроль доступа на объект, информационную безопасность, комплекс мер по противопожарной защите, охранную сигнализацию и видео наблюдение. Прежде всего, устанавливаемый комплекс средств и систем защиты должен соответствовать возможной угрозе. Невозможно исключить все возможности нанесения ущерба, хотя бы по финансовым соображениям.

Используемая аппаратура не должна создавать дополнительных препятствий и больших затруднений нормальной работе гостиницы: ни обслуживающему персоналу, ни гостям. Излишняя секретность, жесткий режим, постоянная демонстрация охраны и подозрительности может отпугнуть клиентов и лишить отель имиджа «открытого дома».

Система должна быть сбалансированной, т.е. средства защиты должны распределяться по возможности равномерно в соответствии с важностью защищаемых зон.

Все применяемые меры и средства не должны создавать дополнительную опасность для здоровья и жизни гостей и сотрудников гостиницы. Это касается в первую очередь обеспечения экстренной эвакуации при чрезвычайных обстоятельствах.

Обеспечение безопасности гостиницы осуществляется на основании следующих принципов:

·        личная ответственность клиента за свою безопасность;

·        ответственность администрации гостиницы за личную безопасность клиента и его имущество;

·        ответственность администрации гостиницы за обеспечение безопасности служащих и имущество компании.

Основным инструментом, обеспечивающим безопасность средств размещения, является “План мероприятий по обеспечению защиты и безопасности клиентов, сотрудников и собственности предприятия”.

Один из руководящих сотрудников, как правило, главный инженер, официально назначается ответственным за выполнение и обновление плана мероприятий по обеспечению безопасности и его соответствием текущим требованиям данного предприятия размещения.

Наиболее часто встречающиеся проблемы в гостиницах — мелкие кражи и низкий уровень санитарии, но важнейшим фактором, представляющим угрозу для жизни клиентов, остается пожар.

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. [18]

К организационным мерам относятся:[29]

·        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.

Необходимо особо отметить, что большую (возможно, главную) опасность для гостиницы представляет возможность пожара, случайного или умышленного поджога, что также требует разработки и внедрения адекватных организационно — технических мер противодействия и является одной из важнейших составляющих комплексной системы безопасности.

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).

·        Среди мер по реализации разработки тактико-организационных мер должно быть уделено особое внимание. В рамках разработки указанных мер необходимо глубокое изучение мирового опыта эксплуатации гостиничных учреждений и работы служб безопасности, данных статистики правонарушений, консультационное взаимодействие со специалистами государственных служб охраны порядка, пожарной безопасности, силовых ведомств.   .3 Современные средства безопасности в гостинице

Выделяют основные подсистемы комплекса технических средств безопасности и средства их интеграции в единую глобальную систему.[13,14,15,16]

Система пожарной безопасности.

Основными задачами системы пожарной безопасности являются:

·        эффективное и своевременное обнаружение очага возгорания с точным указанием места;

·        автоматическое оповещение службы безопасности, всех сотрудников и гостей гостиницы (а, возможно и службы городской пожарной охраны) о возгорании;

·        принятие мер по тушению пожара, предотвращению распространения огня и дыма, дымоудалению;

·        организация эвакуации людей из горящего здания, включая разблокировку всех дверей и лифтов, включение светозвуковых указателей, блокировку лифтов.

В рамках организационно технических мер необходимо оснащение гостиницы пожарным инвентарем и поддержание его в рабочем состоянии.

Система пожарной сигнализации.

Назначение: эффективное и своевременное обнаружение очага возгорания с точным определением места, оповещение сотрудников службы безопасности, городской службы пожарной охраны, инициирование (подача сигнала на включение отключение) прочих систем, документирование информации.

Построение: для обнаружения факта возгорания используются различные типы пожарных датчиков (извещателей):

·        дымовые (оптические, ионизационные, радиоизотопные, линейные и др.). Используются в наиболее важных, пожароопасных зонах, а при возможности во всех помещениях;

·        тепловые, магнитные, с применением легкоплавких материалов, термометрические и пр. Используются в менее ответственных зонах и как вспомогательные;

·        ручные сигнализаторы пожара. Располагаются, как правило, вблизи запасных пожарных выходов, в местах курения и т.д.

·        комбинированные тепло дымовые датчики.

Все датчики могут быть адресными (точное определение места возгорания) или безадресными (определение места с точностью до номера шлейфа, как правило, несколько помещений или целый этаж).

Информация от датчиков собирается центральной станцией пожарной сигнализации, выполняющей функции контроля состояния и работоспособности датчиков, шлейфов исполнительных устройств, оповещения, передачи информации, инициирования и документирования информации. Функции центральной станции могут выполнять:

·        специализированный пожарный приемно-контрольный прибор или многофункциональный приемно-контрольный прибор системы пожарной, охранной и тревожно вызывной сигнализации (при автономной или полуавтономной организации системы безопасности);

·        модули (концентрирования информации, отображения, интерфейса, и др.) интегрированной системы безопасности;

·        система визуально-звукового оповещения.

Назначение: экстренное оповещение гостей и сотрудников гостиницы о возникновении пожара или другой экстремальной ситуации, указание путей скорейшей безопасной эвакуации, выдача прочей экстренной информации.

Построение: для оповещения используются специализированные громкоговорители, световые табло с фиксированными надписями («Пожар», «Выход» и т.п.), пиктограммами или светодиодные табло. Сигнал на включение средств оповещения подается либо автоматически центральной станцией пожарной сигнализации, либо оператором системы безопасности. Аналогично, передаваемая через громкоговорители аудиоинформация может либо произноситься через микрофон оператором, либо быть предварительно записана на магнитофон или в ПЗУ компьютера и передаваться автоматически.

Отметим, что современные мощные интегрированные системы пожарной безопасности включают развитые интеллектуальные системы оповещения, формирующие звуковые и визуальные сообщения в зависимости от конкретной ситуации (конкретного места загорания, размеров территории, охваченной огнем, времени, прошедшего с момента возгорания и т.п.), что обеспечивает наибольшую эффективность эвакуации и безопасность.

Система пожаротушения.[17]

Назначение: автоматическое тушение очага возгорания, предотвращение распространения пожара.

Построение:

Возможны следующие варианты:

·        по принципу пожаротушения:

·        спринклерное пожаротушение (самый дешевый вариант при условии глобальной реконструкции здания);

·        аэрозольное или порошковое пожаротушение;

·        газовое пожаротушение (высокая эффективность, не наносит вреда интерьеру);

·        по принципу организации системы:

·        автономные пожаротушащие модули со встроенными пожарными датчиками;

·        команда на включение пожаротушащего модуля подается центральной пожарной станцией или интегрированной системой безопасности.

Во втором случае за счет использования интеллектуальных возможностей системы уменьшается вероятность ложной тревоги, возможна реализация превентивного включения модулей, расположенных в соседних помещениях.

Управление системой вентиляции и дымоудаления.

Назначение: Предотвращение распространения дыма и огня от очага возгорания по лифтовым и вентиляционным шахтам и трубам, удаление дыма из помещений.

Построение: Включаются подсистемы:

·        дымоудаления: Центральная станция пожарной сигнализации формирует сигналы, запускающие соответствующие электродвигатели вентиляционной системы;

·        предотвращение распространения дыма: Центральная станция пожарной сигнализации формируют сигналы, управляющие приводами заслонок вентиляционной системы, запускает электродвигатели турбин, создающих повышенное давление в лифтовых шахтах.

Отметим, что наиболее сложные интегрированные комплексы (такие, как например, система фирмы Honeywell) полностью включает в свой состав системы вентиляции (электродвигатели, вентиляционные турбины, заслонки и пр.), что повышает эффективность противопожарной защиты

Система разблокировки выходов.

Назначение: При обнаружении системой пожарной сигнализации очага возгорания строго необходимой является автоматическая разблокировка всех дверей. В том числе гостиничных номеров, пожарных и прочих выходов для обеспечения беспрепятственной эвакуации из здания. Также необходимым, с точки зрения пожарной безопасности, является требование автоматического спуска лифтов вниз и полная их блокировка при возникновении пожара.

Построение: Центральная станция пожарной сигнализации формирует сигналы, передаваемые главному контроллеру (локальным контроллерам) системы управления доступом) системы управления доступом, который обеспечивает разблокировку дверей. При этом система разблокировки должна быть интеллектуальной, т.е., например: при локальном возгорании отдельной кладовой хозинвентаря на последнем этаже нет нужды разблокировать все двери здания, и, напротив, при возгорании подобной кладовой, прилежащей к центральной пультовой, реальной становится угроза выхода из строя всей системы в целом и так как дальнейшее развитие событий зачастую непредсказуемо, а рассчитывать надо на худшее, может быть необходима глобальная моментальная разблокировка всех дверей.

Сигналы также передаются контроллерам, управляющими лифтами (во многих системах доступа предусмотрены контроллеры лифтов) для их спуска и блокировки

Система охранной сигнализации.[23]

Назначение: эффективное и своевременное обнаружение факта несанкционированного 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.

Построение: 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:[23]

·        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)

·        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 приемно-контрольный прибор систем пожарной, охранной и тревожно-вызывной 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.[16]

Назначение: 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.

Построение: 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.[34,38]

Назначение: обеспечение беспрепятственного санкционированного 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.

Построение: 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 том или ином этаже.

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;

·        штрих-кодовые 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.[22]

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.

Отметим, что 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.[22] 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.

Отметим в заключение, что современные системы управления доступом имеют настолько большое количество разнообразных функций, что только перечисление их выходит за рамки настоящей Концепции.

Система телевизионного наблюдения.[34,37]

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

Отметим, что во всех современных концепциях безопасности общепризнанным считается положение о высокой эффективности применения систем телевизионного наблюдения.[14] Поэтому практически все комплексы технических средств безопасности крупных объектов, установленные в последние годы за рубежом, оснащаются мощными системами телевизионного наблюдения. 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 (черно-белыми 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.

Часто применяемые, относительно данной задачи, приборы и устройства, для организации системы телевизионного наблюдения:[14]

·        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:

·        о факте прибытия и убытия, времени проживания, распорядке дня, посетителях и телефонных абонентах клиента;

·        о содержании ведущихся клиентом переговоров (в номере или в специально выделенных комнатах);

·        информация, обрабатываемая с применением клиенту или гостинице оргтехники (персональный компьютер, пишущая машинка, электронная записная книжка и т.п.).

Информация, обсуждаемая или обрабатываемая с применением технических средств во время совещаний в специально выделенных помещениях.

Коммерческая тайна.[6]

Коммерческую тайну о деятельности отеля могут составлять сведения об отдельных финансовых показателях, о системе деловых связей, сведения по клиентам, данные по кадрам, сведения по организации охраны и противопожарной безопасности.

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.

Противоаварийный контроль систем жизнеобеспечения здания (газ, вода, электричество).

Назначение: контроль и блокирование в случае аварии (пожара, стихийного бедствия, угрозы теракта) систем жизнеобеспечения гостиничного комплекса.

Построение: существует значительное количество вариантов, рассмотрение которых выходит за рамки настоящей Концепции.

Функции контроля и блокировки систем жизнеобеспечения здания являются стандартными для крупных интегрированных комплексов, 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.

Сформулируем 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 течение, по меньшей мере, двух часов.

Система оперативной связи.

Назначение: 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 для обеспечения оперативной связи.

Укрепленность здания гостиницы.[18]

Назначение: 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.

Вывод

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.

Например: Все гостиничные номера можно оснастить специализированными пультами, связанными с общим комплексом автоматизации здания, обеспечивающими управлением освещением, радиоприемником, телевизором, вызов горничной, техника, передачу тревожного сигнала в службу безопасности, просьбу о медицинской помощи и т.п.; выносное табло такого пульта может отражать надписи типа «Просьба не беспокоить» или «Уберите, пожалуйста, мой номер». В качестве такого пульта, имеющего, однако, меньший набор функций, может быть использовано, например, кодонаборное устройство системы управления доступом.

Кроме того, менеджер гостиницы, горничные, техники всегда смогут иметь полную информацию о жизнедеятельности здания: свободен или занят любой номер, в каком состоянии находится система жизнеобеспечения и т.п., что значительно облегчит их работу.

Полная компьютеризация поможет автоматизировать многие процессы учета.

Возможны другие варианты применения системы комплекса технических средств безопасности в целях повышения качества гостиничного обслуживания, облегчения труда сотрудников гостиницы.  
2. Анализ уровня обеспечения безопасности в гостинице ООО «Новотель» «Калуга Плаза»   .1 Общая характеристика гостиницы «Калуга Плаза»

Гостиница «Калуга Плаза» была построена в 2011г. и предназначена для предоставления основных и дополнительных услуг. Гостиница «Калуга Плаза» расположена в 5-ти минутах езды от центра города, на 2-ом Тульском переулке, д.1.

«Калуга Плаза» представляет из себя комплекс зданий и прилегающую территорию с зонами отдыха и автостоянкой.

Основным зданием комплекса является трех этажное здание, на первом этаже которого располагаются административные помещения, служба приема и размещения, а также несколько гостевых номеров. Два других этажа отведены для номеров и конференц-зала. Гостиница располагает 1, 2 и 3 местным благоустроенными номерами различной категории комфортности, оснащенными телефоном, телевизором, холодильником и системой автономного кондиционирования. В номерах имеется возможность пользоваться беспроводным выходом в Интернет (Wi-Fi). Номера отвечают всем современным требованиям индустрии гостеприимства, обставлены современной мебелью, в каждом номере имеется ванна или душ. Для постояльцев гостиницы организовано питание в ресторане, который находится в гостинице «Калуга — Плаза».

К этому зданию пристроен двухэтажный корпус с номерами категории люкс и рестораном на 90 посадочных мест. Также в комплекс «Калуга Плаза» входят двух этажный корпус с саунами, бассейном и спа-центром.

Удобное расположение, возможность добраться из любой точки города на маршрутном такси, высокий уровень обслуживания, чистота и уют, доброжелательный микроклимат, приветливый персонал выгодно отличают «Калуга Плаза» от других гостиниц города. В гостинице любят останавливаться иностранные туристы из многих стран мира, в том числе из Франции, Англии, США, спортсмены и артисты, военные и работники образования, приезжающие в город на совещания. У многих постоянных клиентов есть любимые номера, где они отдыхают в комфорте и уюте.

Недалеко от гостиницы находятся художественный и краеведческий музеи, Дворец спорта, областной Драматический театр и кинотеатр, парк отдыха, множество торговых точек.

Организационно-правовая форма гостиничного предприятия — общество с ограниченной ответственностью. В настоящее время на рынке гостиничных услуг организационно-правовая форма предприятия типа общества с ограниченной ответственностью является наиболее распространенной. [приложение 6]

Целью создания гостиницы является оказание услуг гостиничного комплекса и получение прибыли. Основными видами деятельности гостиницы «Калуга Плаза» являются:

·   оказание услуг гостиничного комплекса по временному проживанию;

·        оказание проживающим в гостиничном комплексе услуг банно-прачечного хозяйства;

·        оказание услуг по охране автотранспорта, принадлежащего проживающим;

·        предоставление услуг питания.

Гостиница «Калуга Плаза» предоставляет клиентам следующие услуги:

·        услуги размещения;

·        обеспечение клиентов питанием;

·        услуги пункта обмена валюты;

·        заказ авиа и железнодорожных билетов;

·        услуги охраняемой автостоянки;

·        вызов такси;

·        услуги прачечной и т.д.

В настоящее время в гостинице имеется 52 номера различных категорий. Общее количество мест составляет 87. Гостиница предлагает услуги размещения различных ценовых категорий. Стоимость номеров варьируется от 3900 до 10200 руб. за сутки. Средняя стоимость номера составляет около 4500 — 6000 руб. за сутки. На стоимость номера оказывают влияние следующие факторы: категория предоставляемого номера; месторасположение номера. Существует также система скидок в зависимости от количества гостей в группе. В стоимость проживания включен завтрак в ресторане на первом этаже гостиницы.

Таким образом, гостиница «Калуга Плаза» функционирует на рынке гостиничных услуг города Калуги и является одной из крупных предприятий гостиничного сервиса. Гостиница оказывает услуги по размещению гостей города Калуга. Кроме того, клиентам предоставляется ряд дополнительных услуг. Однако для того, чтобы определить эффективность деятельности гостиницы, необходим более тщательный анализ предприятия по основным направлениям деятельности.

Гостиница осуществляет предоставление услуг по договорам с организациями, фирмами, предприятиями по заявкам на размещение, а также по свободному поселению при наличии свободных мест. Гостиница предоставляет свои услуги гражданам России, СНГ и стран ближнего и дальнего зарубежья, предъявившим документ, удостоверяющий его личность. Граждане ближнего зарубежья заселяются в гостиницу при предъявлении национального паспорта и миграционной карты. При заселении иностранных граждан администратор или портье обязан заполнить данные статистической отчетности с указанием фамилии, имени, номера визы, срока действия визы, цели поездки и страны проживания. При оформлении проживания в гостинице гость обязан ознакомиться с порядком проживания в гостинице, правилами противопожарной безопасности, правилами пользования электроприборами. Оформление гостей, прибывающих в гостиницу и убывающих из нее, производится круглосуточно.

Гостиница «Калуга Плаза» оказывает как основные, так и дополнительные услуги гостям города Калуга. Основными услугами гостиничного комплекса являются услуги размещения.

Санузлы номеров оборудованы душевыми кабинами, умывальники, унитазы. В номерах повышенной категории комфортности — ванные, умывальники, унитазы.

Организационная структура гостиницы характеризуется совокупностью рабочих мест, должностей, органов управления и производственных подразделений, форм их взаимосвязи, обеспечивающих достижения стратегических целей гостиницы.

Таблица 2.1 Структура номерного фонда

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Этаж | стандарт | премиум стандарт | твин | Гранд де люкс | Гранд романтик | Гранд люкс | Гранд фэмили | Всего | Мест |
| 1 этаж | — | 6 | 5 | — | — | — | — | 16 | 22 |
| 2 этаж | 7 | 8 | — | 6 | 1 | 1 | 1 | 19 | 48 |
| 3 этаж | 17 | — | — | — | — | — | — | 17 | 17 |

В рамках организационной структуры предприятия выделяют две основные составляющие: структура управления и обслуживающая (производственная) структура.

Структура производственная предопределяет разделения экономического объекта на части, элементы по производственно-технологическим принципам (бронирование, размещение, оплата услуг).

Для структуры управления гостиницы характерны звенья (отделы), уровни (ступени) управления.

К звеньям управления предприятия относятся структурные подразделения, отдельные специалисты, выполняющие функцию управления, либо их часть, менеджеры, осуществляющие регулирование и координацию деятельности нескольких структурных подразделений.

Общие решения стратегического характера принимаются владельцами гостиницы и генеральным директором.[приложение 4]

Посредником между владельцами предприятия и управленческим персоналом является генеральный директор, который выполняет огромное количество задач, например, принятие ориентированных на выбранный сегмент рынка решений, направленных на удовлетворение потребностей клиентов, определение общих направлений политики гостиничного предприятия в рамках поставленных целей, задач, в том числе проведение финансовой политики, к которой могут быть отнесены такие вопросы, как определение лимитов на содержание персонала, на административные и хозяйственные нужды.

В гостинице «Калуга Плаза» применяется одна из простейших структур линейная. При линейной структуре управления гостиницей производство услуг и их реализация четко разграничены: одни подразделения занимаются подготовкой услуг, другие — обслуживанием, третьи — продажей услуг.

При любой модели управления главная задача руководителя — обеспечить необходимые ресурсы и координированность усилий работников индустрии гостиничного сервиса на выполнение намеченных целей.

Таким образом, в рамках определенной организационной структуры, введенной на данном предприятии, осуществляется процесс управления единым хозяйственным механизмом.

Организация работы службы приёма и размещения.

Службу приема часто называют «сердцем», или «нервным центром», гостиницы. С этой службой гость контактирует больше всего, сюда же он обращается за информацией и услугами во время своего пребывания в гостинице.

Контроль за обеспечением безопасности в гостинице осуществляет служба безопасности, которой руководит начальник службы безопасности.

К важнейшим функциям службы приема относится приветствие гостя и выполнение необходимых формальностей при его размещении. От того, как примут гостя, как его поприветствуют, как быстро будут выполнены необходимые формальности, во многом зависит первое, часто самое сильное впечатление от гостиницы в целом.

Возглавляет службу обслуживания администратор, которому подчинены дежурные по этажам. Администратор является первым в цепочке взаимодействия с гостями, он встречает и размещает гостей. Принимает оплату за проживание, решает возникающие вопросы. Расчёт производится у стойки администратора. [приложение 5]

В размещении согласовывают категорию номера, наличие удобств, вид оплаты, цену, срок пребывания, дату отъезда. К функции службы приема и расчетной части относятся также распределение номеров и учета свободных мест в гостинице, выписка счетов и производство расчетов с клиентами.

Клиенты могут забронировать номер по телефону, электронной почте, по факсу. Так же на стойке администратора имеется тревожная кнопка для вызова, в случае ЧП, сотрудников правоохранительных органов.   .2 Анализ систем видеонаблюдения и видеоконтроля

Одним из наиболее важных компонентов в безопасности гостиничного комплекса «Калуга Плаза» является высокоинформативная и надежная система видеонаблюдения.

Системы видeoнaблюдeния позволяют обеспечивать не только непрерывный оперативный контроль за помещениями и территорией, но и oбнapуживaть втopжeниe в зaдaнныe oблacти пpocтpaнcтвa, ocущecтвлять видeoзaпиcь тpeвoжныx coбытий, или нeпpepывную видеорегистрацию происходящего.

Системы видеонаблюдения гостиничного комплекс «Калуга Плаза» включают в себя такое оборудование, как видеорегистраторы длительной записи, видеокамеры, мониторы, поворотные устройства и многое другое. Какие именно устройства и в каком количестве будут составлять систему видеонаблюдения и видеорегистрации, зависит от того, для какого объекта эта система видеонаблюдения будет использоваться.

В данном случае как внутри помещении так и снаружи гостиничного комплекса «Калуга Плаза» установлены камеры фирмы BOSCH.

Для наружного видеонаблюдения используются EX85 инфракрасные мегапиксельные IP-камеры: Дневной датчик 3,1 мегапикселя, ночной датчик 1,3 мегапикселя, ночное видение на уровне обнаружения на расстоянии 128 м, проверенная в эксплуатации всепогодная конструкция IP67, новаторская технология Bit-Reduce сокращает требования к пропускной способности сети, технология Black Diamond способствует устранению «пересветов» на переднем плане и «недодержанных» участков на заднем плане.

Важнейшим качеством телевизионных систем видеонаблюдения при охране объектов является возможность осуществления регистрации и документирования в течение длительного времени видеонаблюдения событий, происходящих на охраняемых объектах. Для этого используют видеозапись, которые могут работать как в непрерывном режиме, так и в режиме покадровой записи с заданным интервалом времени между кадрами, с обязательной записью текущего времени и даты. При воспроизведении такой записи возможен многократный ретроспективный контроль всей обстановки в наблюдаемых зонах, детальное изучение тревожной ситуации в наблюдаемой зоне с установлением времени происходящих событий.

Таким образом, системы видеоконтроля — это системы видеонаблюдения с видеозаписью оказывают огромную помощь службе безопасности в объективной оценке обстановки на объекте, идентификации объектов контроля, а так же позволяют оценить качество работы операторов.   .3 Анализ уровня пожарной безопасности гостиницы «Калуга Плаза»

В соответствии с Федеральным законом «О пожарной безопасности» и Правилами пожарной безопасности в Российской Федерации [17] (далее — Правила) устанавливают требования пожарной безопасности, обязательные для применения и исполнения органами государственной власти, органами местного самоуправления, организациями независимо от их организационно-правовых форм и форм собственности (далее — организации), их должностными лицами, предпринимателями без юридического образования, гражданами Российской Федерации, иностранными гражданами, лицами без гражданства (далее — граждане) в целях защиты жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества, охраны окружающей среды.

Пожарная безопасность — состояние объекта, характеризуемое возможностью предотвращения возникновения и развития пожара, а также воздействия на людей и имущество опасных факторов пожара. Пожарная безопасность объекта должна обеспечиваться системами предотвращения пожара и противопожарной защиты, в том числе организационно-техническими мероприятиями.

Система пожарной сигнализации — это сложный комплекс технических средств, который реагирует на задымление, изменение температуры воздуха при помощи специальных датчиков. Датчики посылают сигнал тревоги на приемно-контрольный прибор, после чего сигнал моментально передается на пульт пожарной охраны.

Противопожарная профилактика — это комплекс мероприятий, направленных на обеспечение безопасности жизни людей, сохранность зданий и имущества, предупреждение пожаров и создание условий для успешного их тушения.

Противопожарная безопасность в гостиницах обеспечивается соблюдением требований, изложенных в правилах пожарной безопасности. В них предусматривается целый ряд профилактических мер, круг служебных обязанностей должностных лиц, организация эвакуации людей и действия персонала во время пожара.

Для гостиниц очень важно содержать в надлежащем порядке пути эвакуации [17,п.52], средства противопожарной защиты [17,п.53] (системы дымоудаления, подпора воздуха в лифтовых шахтах и перед лестничной клеткой, установки пожарной автоматики внутреннего пожарного водопровода).

В коридорах, на лестничных клетках, дверях, ведущих к путям эвакуации или непосредственно на улицу, должны находиться символические изображения знака “выход” — открытая дверь с силуэтом бегущего человека и стрелка, указывающая его движение к выходу.

В каждом номере применительно к структуре здания гостиницы должен быть поэтажный план индивидуальной эвакуации [17,п.125] вывешивать его следует в удобном месте.

Для обеспечения должного уровня безопасности проживания гостиницы должны быть оборудованы системой экстренного оповещения гостей на случай вынужденной эвакуации [17,п.102]. Наиболее частые причины возникновения пожаров в гостиницах неосторожное обращение с огнем, неисправность электросетей, электрооборудования, нарушения технологического процесса и правил эксплуатации оборудования для приготовления пищи, несоблюдение мер пожарной безопасности при ремонтных и электросварочных работах, а также часты случаи загораний от неисправных телевизоров, установленных в номерах.

Принятые на работу в гостиницу проходят инструктаж по пожарной безопасности [17,п.126] — знакомятся с действующими в гостинице правилами и инструкциями, регламентирующими поведение персонала, средствами тушения пожаров (работа с пожарным краном и огнетушителями разного вида), с работой противопожарной сигнализации и автоматики. Периодически в гостиницах проводятся учебные пожарные тревоги, цель которых — выработать навыки поведения персонала в аварийной ситуации.

Как правило, случаи возгораний происходят в позднее и ночное время. Дежурный персонал, заступая на работу, обязан в первую очередь проверить наличие первичных средств пожаротушения, не загромождены ли чем-либо эвакуационные проходы, коридоры, холлы и лестничные клетки, убедиться в возможности быстрого и беспрепятственного открывания дверей всех эвакуационных выходов.

При возникновении пожара дежурный администратор (или другие должностные лица) обязан немедленно сообщить о пожаре в пожарную охрану, принять все меры, зависящие от него, к эвакуации людей из номеров, использовать все средства оповещения о пожаре.

Чрезвычайно важно для обеспечения строгого противопожарного режима в гостинице напомнить гостю о соблюдении противопожарных правил.

В каждой гостинице имеется памятка для проживающих [17,п.127], в которой излагаются основные рекомендации о мерах пожарной безопасности и правила поведения при пожаре.

В соответствии с федеральным законом «О пожарной безопасности» [4] и правилами пожарной безопасности для гостиниц [17,п.129] обслуживающий персонал обеспечен индивидуальными средствами фильтрующего действия для защиты органов дыхания, которые хранятся непосредственно на рабочем месте обслуживающего персонала.

На территории Российской Федерации в 2011 году произошло 168205 пожаров, прямой ущерб от которых составил 16,882 млрд. рублей. На пожарах погибло 11962 человека (над этим надо задуматься, это не просто цифры), 12425 получили травмы. Снижение по количеству пожаров составило 6,3%, по количеству погибших 8,5%, количество травмированных снизилось на 5,3 %. Материальный ущерб увеличился на 15,9 %. На ликвидацию загораний пожарные подразделения выезжали 43613 тыс. раз.

В организациях и ЗАТО, охраняемых специальными подразделениями ФПС МЧС России, в 2011 году зарегистрировано 926 пожаров с ущербом 30,721 млн. руб. На пожарах погибло 54 человека, 103 травмировано. Огнем уничтожено 224 строения, 52 единицы автотракторной и другой техники. На пожарах спасено 969 человек и материальных ценностей на сумму 202,137 млн. руб.

Обстановка с пожарами в охраняемых организациях: (Таблица 1)

В организациях, охраняемых специальными подразделениями ФПС МЧС России, в 2011 году зарегистрировано 33 пожара (3,5% от общего количества пожаров), с ущербом 764 тыс. руб. На пожарах травмировано 7 человек.

Таблица 2.2 — Сведения о пожарах по причинам возникновения

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Количество пожаров | | | +/- %АППГ | Погибло людей | | | +/- %АППГ |
|  | 2010 | 2011 | |  | 2010 | 2011 | |  |
| Умышленное уничтожение имущества | 251 | | 237 | -5,6 | 1 | |  | -1 человек |
| Неисправность производственного оборудования, нарушение технического процесса | 8 | | 6 | -25,0 |  | |  | 0,0 |
| Нарушение ПУиЭ электрооборудования | 160 | | 133 | -16,9 | 10 | | 7 | -30,0 |
| Нарушение ПУиЭ печей | 77 | | 58 | -24,7 | 3 | | 2 | -33,3 |
| Нарушение ПУиЭ теплогенерирующих агрегатов и установок | 5 | | 2 | В 2,5 раза |  | |  | 0,0 |
| Неосторожное обращение с огнем | 351 | | 348 | -0,9 | 34 | | 44 | 29,4 |
| В том числе неосторожное обращение с огнем детей | 30 | | 34 | 13,3 |  | | 1 | +1 человек |
| Нарушение ПУиЭ транспортных средств | 64 | | 49 | -23,4 | 1 | |  | -1 человек |
| Нарушение ППБ при проведении газо-электросварочных работ | 11 | | 11 | 0,0 |  | |  | 0,0 |
| Неустановленные причины | 32 | | 39 | 21,9 | 1 | | 1 | 0,0 |
| Нарушение ППБ при проведении огневых работ | 13 | | 9 | -30,8 |  | |  | 0,0 |
| Итого | 1017 | | 926 | -8,9 | 50 | | 54 | 8,0 |
|  |  |  |  |  |  |  |  |  |

Гибели людей не допущено (2010г. — 42 пожара, ущерб — 42619 тыс. руб., без гибели, травмировано 7 человек).

По сравнению с 2010 годом количество пожаров уменьшилось на 21,4%, количество травмированных не изменилось, материальный ущерб уменьшился в 55,7 раза.

По сравнению с 2010 годом, количество пожаров уменьшилось на 8,9% (2010г. — 1017 пожаров). Увеличилось количество погибших людей на пожарах на 8% (2010г. — 50чел.), число травмированных на 8,4% (2010г. — 95 чел.). Ущерб от пожаров снизился в 2,2 раза (2010г.-66,816 млн. руб.).

Таблица 2.3 — Основные причины пожаров

|  |  |
| --- | --- |
| Нарушения правил устройства и эксплуатации электрооборудования | 14% (133 случая) |
| Неосторожное обращение с огнем | 37%(348 случаев), в том числе неосторожность при курении — 18% (174 случая) |
| Поджоги | 25% (237 случаев) |

На пожарах, причиной которых стало неосторожное обращение с огнем, погибло 44 человека (таблица 2): (81% от общего числа пожаров), в т.ч. по неосторожности при курении 35 человек, причем по сравнению с 2010г. Количество погибших по неосторожности при курении выросло на 20,7%.

В связи с чередой трагических происшествий случившихся в нашей стране за последнее время и повлекшие смерть большого количества людей руководством комплекса еще на моменте проектирования здания подрядчикам были поставлены строгие требования по соблюдению мер пожарной безопасности — действия по обеспечению пожарной безопасности, в том числе по выполнению требований пожарной безопасности, такие как: необходимое количество пожарных выходов с лестничными маршами, ширина и высота проема дверей и окон.

В гостинице «Калуга Плаза» система пожарной безопасности обеспечивает: эффективное и своевременное обнаружение очага возгорания с точным указанием места; оповещение службы безопасности, всех сотрудников и посетителей гостиницы (и службы пожарной охраны тоже) о пожаре; принятие мер по предотвращению распространения огня и дыма, дымоудалению; организацию эвакуации людей из горящего здания, включение светозвуковых указателей.

Для обнаружения факта возгорания используются типы пожарных датчиков:

извещатель пожарный дымовой оптико-электронный адресно-аналоговый;

ручные сигнализаторы пожара — располагаются вблизи запасных пожарных выходов, в местах курения и т.д.

Для оповещения используются специализированные громкоговорители, световые табло с фиксированными надписями «Выход».

При эксплуатации гостиницы соблюдаются требования пожарной безопасности [17]:

·        разработана инструкция о мерах пожарной безопасности

·        в номерах вывешены планы эвакуации на случай пожара

·        всех прибывающих в гостиницу граждан ознакомляют под роспись

·        памятка о мерах пожарной безопасности выполнена на нескольких языках

·        во всех помещениях на видных местах вывешены таблички с указанием номера телефона вызова пожарной охраны

·        распорядительным документом установлен соответствующий противопожарный режим (определены и оборудованы места для курения, определены места и допустимое количество единовременно находящихся в помещениях сырья, полуфабрикатов и готовой продукции, установлен порядок уборки горючих отходов и пыли, определен порядок обесточивания электрооборудования в случае пожара и по окончании рабочего дня)

·        определен порядок и сроки прохождения противопожарного инструктажа и занятий по пожарно-техническому минимуму, а также назначены ответственные за их проведение.

Перечень документов по пожарной безопасности:[7]

·        Приказ об установлении противопожарного режима.

·        Общеобъектовая инструкция о мерах пожарной безопасности ИПБ-001.

·        Инструкция о мерах пожарной безопасности при проведении мероприятий с массовым пребыванием людей ИПБ-002.

·        Инструкция по содержанию и применению первичных средств пожаротушения ИПБ-003.

·        Инструкция по проведению противопожарного инструктажа ИПБ-004.

·        Инструкция по техническому обслуживанию пожарной сигнализации и системы оповещения о пожаре ИПБ-005.

·        Программы проведения противопожарного инструктажа и обучения пожарно-техническому минимуму.

·        Порядок действий работников при обнаружении пожара.

·        Места размещения огнетушителей — ресторан.

·        Места размещения огнетушителей — гостиница.

·        Схема оповещения руководящего состава о пожаре и ЧС.

·        Должностные обязанности генерального директора.

·        Должностные обязанности ответственного по пожарной безопасности.

·        Должностные обязанности руководителей структурных подразделений.

·        Расчет первичных средств пожаротушения (огнетушителей).

·        Договор на противопожарную обработку деревянных конструкций.

·        Договор на техническое обслуживание системы автоматической пожарной сигнализации и системы оповещения людей о пожаре.

·        Приказ об окончании учебного сбора по программе пожарно-технического минимума, копии удостоверений обученных лиц.

·        Планы эвакуации: на каждом этаже, в каждом номере.

·        Памятка о правилах пожарной безопасности для проживающих в гостинице.

·        Приказы по пожарной безопасности.

·        Журналы: учета огнетушителей, технического обслуживания огнетушителей, вводного противопожарного инструктажа, противопожарного инструктажа на рабочем месте, технического обслуживания пожарной сигнализации и системы оповещения о пожаре, отработки планов эвакуации.

Для соблюдения всех противопожарных норм с гостиничным комплексом «Калуга Плаза» был заключен договор с компаниями имеющими лицензию на данный вид деятельности, на установку и обслуживание систем противопожарной безопасности. Все датчики, приборы и программное обеспечение относящиеся к противопожарной безопасности имеют необходимые сертификаты и лицензии.   .4 Анализ уровня информационной безопасности

Информационная безопасность предприятия — это защищенность информации, которой располагает предприятие (производит, передает или получает) от несанкционированного доступа, разрушения, модификации, раскрытия и задержек при поступлении. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Главной целью любой системы информационной безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов Заказчика от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта. Другой целью системы информационной безопасности является повышение качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов.

Достижение заданных целей возможно в ходе решения следующих основных задач:

·        отнесение информации к категории ограниченного доступа (служебной тайне);

·        прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

·        создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;

·        создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;

·        создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения информационной безопасности на достижение стратегических целей.

Модель построения системы информационной безопасности (Рисунок 1).

При выполнении работ можно использовать следующую модель построения системы информационной безопасности (рис. 1), основанную на адаптации ОК (ISO 15408) [8] и проведении анализа риска (ISO 17799)[9].

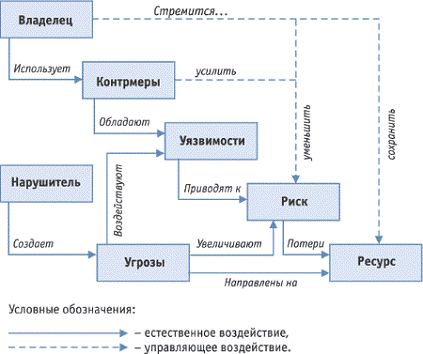


Рис. 1 Модель построения системы информационной безопасности предприятия

Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарту ISO/IEC 15408 «Информационная технология — методы защиты — критерии оценки информационной безопасности», стандарту ISO/IEC 17799 «Управление информационной безопасностью», и учитывает тенденции развития отечественной нормативной базы (в частности, Гостехкомиссии РФ) по вопросам информационной безопасности.

Представленная модель информационной безопасности — это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Гостиница оборудована серверным помещением. Серверная комната (серверное помещение или просто серверная) — выделенное технологическое помещение со специально созданными и поддерживаемыми условиями для размещения и функционирования серверного и телекоммуникационного оборудования.

Для этих целей было закуплено серверное оборудование фирмы APC:[40]

ИТ-шкаф с базовой функциональностью и возможностью AR3357. Самые универсальные в мире монтажные шкафы для требовательных ИТ-сред. NetShelter SX представляет новое поколение решений APC в области шкафов-стоек, созданное с учетом отзывов заказчиков, собиравшихся в течение десяти лет, и современных тенденций рынка информационных технологий в области серверов и сетевых систем с высокой удельной мощностью. NetShelter SX представляет собой надежное решение для монтажа критически важного стоечного оборудования, в котором особое внимание уделяется охлаждению, распределению питания, управлению кабелями и мониторингу микроклимата.

Источники бесперебойного питания Smart-UPS On-Line. Универсальный ИБП, разработанный в расчете на самые неблагоприятные качественные показатели электросети, какие только встречаются в нашем мире.

В ИБП Smart-UPS On-Line с поддержкой высокой энергетической плотности реализована топология постоянно действующего двойного преобразования для защиты серверов, сетей голосовой связи и передачи данных. Поддерживающий нагрузки от 1 до 20 кВА в трансформируемой стоечно-вертикальной конструкции. Недавно представленные модели мощностью 15 и 20 кВА позволяют подключать энергоемкие блейд-серверы или стойки с высокой плотностью компоновки оборудования. Если ответственные системы нуждаются не в минутах, а в часах автономной работы, ИБП Smart-UPS On-Line может комплектоваться совместимыми батарейными блоками, соответствующими таким жестким требованиям ко времени автономной работы. Прилагаемое ПО управления PowerChute поддерживает безопасное автоматическое завершение работы сетевых операционных систем. Все модели мощностью 5 кВА и выше комплектуются интегрированной платой сетевого управления для дистанционного контроля (опция в моделях мощностью менее 5 кВА). Вся линия ИБП Smart-UPS On-Line представляет особый интерес для требовательных заказчиков, которым важны такие характеристики, как очень широкое окно допустимого входного напряжения, предельно точная стабилизация выходного напряжения, стабилизация частоты, внутренний байпас и коррекция коэффициента мощности на входе.

Консольный блок для стойки с клавиатурой, мышью и ЖК-монитором Rack LCD Consoles. APC Rack LCD Monitor Keyboard Mouse представляет собой интегрированный комплект из клавиатуры, ЖК-монитора с диагональю 17 дюймов и мыши в компактном конструктиве, позади которого в стойке еще остается место для установки коммутатора консоли. Устройство легко монтируется и требует минимальных затрат на поддержку и сопровождение, что положительно сказывается на совокупной стоимости владения. Сверхтонкий ЖК-экран, сенсорная площадка и простые в установке выдвижные направляющие образуют в совокупности высококачественное, рационализированное решение управления серверами. Rack LCD может использоваться в разнообразных ИТ-средах, от компьютерных залов до крупных выстовочных центров.

Матричные коммутаторы APC KVM Switches. KVM Switches переключатели для серверов спроектированы с учетом требований повышения уровней готовности и администрируемости. Доступ к серверам из любого места помещения и из любой точки мира. Стоечные коммутаторы клавиатуры, монитора и мыши APC дают администратору возможность локального и удаленного доступа на уровне POST и BIOS и управления подключенными серверами Windows, SUN и Linux/UNIX. Коммутаторы клавиатуры, монитора и мыши APC (аналоговые, аналоговые категории 5 и IP-коммутаторы) позволяют использовать один комплект из клавиатуры, монитора и мыши для работы с разными серверами, помогая снизить совокупную стоимость владения за счет экономии пространства и сокращения расходов на оборудование, электроэнергию и кабели. Масштабируемость корпоративного уровня и централизованное управление помогают повысить гибкость и увеличить прибыль на инвестированный капитал. Стоечные коммутаторы клавиатуры, монитора и мыши APC обеспечивают более надежный контроль и уверенность при управлении ИТ-инфраструктурой в центрах обработки данных, компьютерных залах и удаленных филиалах.

Коммутаторы интернет Ethernet Switches. Высокопроизводительная коммутационная технология для поддержки сетевой инфраструктуры. Коммутаторы APC для сетей Ethernet способствуют повышению эксплуатационной готовности, предлагая готовое интегрированное решение, разработанное для архитектуры InfraStruXure. Они помогают добиться снижения совокупной стоимости владения за счет обеспечения быстрой передачи данных при экономных ценовых показателях. Коммутаторы APC для сетей Ethernet в стоечном исполнении помогают сетевым администраторам решать проблемы, связанные с работой сети. Они предназначены для борьбы с перегрузкой каналов связи. Эти коммутаторы могут использоваться везде, где имеется сетевое оборудование: в коммутационных узлах, компьютерных залах и центрах обработки данных любых размеров.

Серверный корпус NR-N4310 (mATX 10×9.6, 2×5.25, 2×3.5″, 2×2.5″, 300mm) черный. Отличное решение для платформы 4U. Конструктив корпуса позволяет устанавливать стандартные материнские платы формата microATX, размером до 9.6″x9.6″. Корпус изготовлен из обработанной прочной стали, что позволяет избежать повреждения рук при сборе сервера. Два мощных вентилятора, обеспечивают прекрасное охлаждение. Наличие большого количества отсеков 3.5″ и 5.25″ даёт широкие возможности для установки HDD, корзин с горячей заменой HDD и других устройств.

Мини АТС Avaya. Коммуникационный сервер Avaya S8300 разработан на базе шлюза G430 и управляющего процессора S8300. Реализация объединяет в себе многофункциональные возможности программного обеспечения MultiVantage ( на коммутаторе Ethernet), и предлагает большие возможности для телефонизации малых и средних офисов на базе локальной сети передачи данных.

Базовыми составляющими шлюза G430 являются:

Шлюз поддерживает до 2-х дополнительных внешних модулей EM200, позволяющих увеличить абонентскую и портовую емкость при расширении телекоммуникационной емкости офиса. Каждый EM200 имеет 2 слота для медиа модулей и присоединяется к шлюзу G430 посредством шины. Шлюз G430 работает под программным обеспечением Avaya AuraTM Communication Manager начиная с версии 5.2, которое устанавливается на серверах Avaya S8XXX.

Медиа шлюз G430 объединяет функции АТС и сети передачи данных. Он позволяет при осуществлении звонка обеспечить пути обхода ТФоП через маршрутизацию данных и VoIP трафика по сети Internet. Шлюз обеспечивает полную поддержку IP и цифровых телефонов Avaya, а также аналоговых устройств сторонних производителей, таких как модемы, факсы и аналоговые телефоны. Шлюз G430 — это масштабируемое устройство, включающее в базовую конфигурацию один блок питания, 256 МБ RAM и одну внутреннюю DSP карту на 20 VoIP каналов. Эта конфигурация может быть расширена путем добавления DSP карт, поддерживающих 10, 20 или 80 VoIP каналов. Кроме того, можно заменить 256 МБ RAM на 512 МБ RAM и использовать дополнительную Compact flash для увеличения количества файлов объявлений с 256 до 1024 и увеличить время объявлений с 45-ти минут до 4-х часов.

Основные возможности медиа-шлюза G430:

·        Два встроенных порта 10/100 Base-T LAN, один 10/100 Base-T WAN порт, два USB порта, сервисные порты, Contact closure adjunct порт, Compact Flash слот для дополнительного хранилища объявлений.

·        DSP ресурсы от 20 VoIP каналов в базовой конфигурации и до 100 каналов при добавлении дополнительных внутренних DSP карт (на 10, 20 и 80 каналов). Поддерживаются кодеки G.711, G.729, and G.726.

·        Поддерживает стандартную локальную выживаемость (SLS) и расширенную локальную выживаемость (ELS) с сервером S8300.

·        Основные свойства маршрутизации включают поддержку протоколов RIP, OSPF и VRRP. К G430 также может подключаться внешнее WAN устройство через фиксированный 10/100 Ethernet WAN router порт, который обеспечивает планирование распределения трафика для согласования скоростей передачи данных с доступной полосой пропускания.

·        Улучшенное качество обслуживания (QoS) включает динамическое управление разрешениями вызовов (Dynamic Call Admission Control) для улучшения использования полосы пропускания и отчет о времени ответа (Respond Time Report) для улучшенного WAN мониторинга.

·        Расширенная защита включает поддержку VPN, SRTP шифрования, SSH/SCP, SNMP v3 поддержку и управление паролями.

·        В данном решении нашли применение также и все возможные модули расширения коммутатора Cajun P330, от 16 портового модуля Ethernet 10/100 и до гигабитного Ethernet и WAN маршрутизатора.

Управляющий процессор телефонии S8300 может работать в режиме основного или резервного процессора системы. Резервный процессор находится в состоянии » холодного» резерва с текущей копией всех установок системы, он начинает действовать в случае потери связи между шлюзом G700 и основным процессором сети (S8300 или S8700) и может управлять не только шлюзами G700, но и обратившимися к нему за регистрацией абонентами IP, для которых этот резервный процессор прописан в списке альтернативного сторожа.

Решение S8300/G430 предлагает высочайшую плотность пользовательских функций в ограниченном объеме плюс поддержку практически всех необходимых коммутационных протоколов и портов.

Сервер работает на программном обеспечении Windows Server 2008 R2. ОС Windows Server 2008 R2 создана на основе завоевавшей признание ОС Windows Server 2008; она расширяет возможности существующих технологий, а также предоставляет организациям новые возможности, повышающие гибкость и надежность серверных инфраструктур. Новые средства виртуализации, веб-ресурсы, усовершенствованные средства управления и возможность интеграции с Windows 7 экономят время, снижают расходы и предоставляют платформу для эффективного динамического управления центрами обработки данных. Windows PowerShell 2.0, службы IIS 7.5, обновленные диспетчер серверов и гипервизор Hyper-V, а также другие мощные средства повышают управляемость систем и позволяют заказчикам быстрее реагировать на изменение требований бизнеса.

Windows Server 2008 R2 защищена антивирусным программным обеспечением Symantec Endpoint Protection. Symantec Endpoint Protection предоставляет не только передовую в отрасли антивирусную защиту, но также основанную на сигнатурах защиту от программ-шпионов. Это решение также обеспечивает предотвращение угроз, что позволяет защитить конечные точки от целенаправленных и неизвестных атак. Оно включает готовые активные технологии, которые автоматически анализируют поведение приложений и сетевых подключений для обнаружения и блокировки подозрительных действий, а также возможности администрирования, позволяющие запретить определенные действия устройств и приложений, которые считаются крайне опасными для организации. Определенные действия можно заблокировать даже исходя из местонахождения пользователя.

Кроме того, обеспечивается защита даже от наиболее сложных, неуловимых для традиционных средств безопасности атак, таких как руткит, эксплойт «нулевого дня» и изменяющиеся программы-шпионы.

Ключевые преимущества Symantec Endpoint Protection:

Комплексная защита — интеграция лучших технологий для предотвращения угроз безопасности даже от самых удаленных новых и неизвестных злоумышленников до их проникновения в сеть. Обнаружение и блокировка злонамеренного программного обеспечения, включая вирусы, червей, троянских коней, программы-шпионы, рекламное ПО и руткиты, осуществляется в режиме реального времени.

Превентивная защита — в новом модуле превентивного поиска угроз Proactive Threat Scan используется уникальная технология Symantec для оценки правильных и неправильных действий неизвестных приложений, которая улучшает обнаружение и уменьшает число ошибочных идентификаций без необходимости создания конфигураций на основе правил.

Лучшее в отрасли выявление угроз — механизмы защиты компании Symantec развивают передовую в отрасли сеть Global Intelligence Network для обеспечения беспрецедентной возможности просмотра всех Интернет-угроз. Благодаря такому выявлению создается защита, ведущая к действиям, и достигается уверенность в сдерживании меняющихся угроз.

Единый агент, единая консоль — объединяет весь спектр технологий безопасности в единого агента и консоль централизованного управления с интуитивным пользовательским интерфейсом, а также средством создания графических отчетов с веб-интерфейсом. Эти компоненты позволяют установить и усилить политики безопасности на предприятии, чтобы обеспечить защиту важных активов. С их помощью упрощается управление, понижается использование ресурсов системы, а при добавлении поддержки Symantec Network Access Control не требуются дополнительные агенты. После приобретения лицензии функции Symantec Network Access Control автоматически включаются на агенте и консоли управления.

Простота развертывания — поскольку требуется только один агент и одна консоль управления, а работа осуществляется с существующими инвестициями организации в ИТ и безопасность, решение Symantec Endpoint Protection обеспечивает простоту реализации и развертывания. Для организаций, которым необходимо привлекать сторонних исполнителей для контроля безопасности и управления, компания Symantec предоставляет службу Managed Security Services, обеспечивающую защиту в режиме реального времени.

Низкая стоимость владения — решение Symantec Endpoint Protection обеспечивает более низкую стоимость владения за счет уменьшения административных расходов, а также расходов, связанных с управлением несколькими продуктами защиты конечных точек. Этот унифицированный подход к безопасности конечных точек упрощает управление и обеспечивает эффективность эксплуатации, за счет единого обновления программного обеспечения и политик, унифицированного и централизованного выполнения отчетов, а также использования единой программы лицензирования и обслуживания.

Простота установки, настройки и управления — решение Symantec Endpoint Protection упрощает включение/отключение и настройку необходимых технологий в соответствии с Вашей средой.

Поддержка Symantec Network Access Control — каждая конечная точка получает поддержку Symantec Network Access Control, что устраняет необходимость развертывания дополнительного программного обеспечения агента конечных точек для контроля доступа к сети.

Повышение эффективности существующих технологий безопасности и ИТ-инвестиций — возможность работы с другими ведущими поставщиками антивирусного ПО, брандмауэров, технологий IPS и инфраструктур контроля доступа к сети. Кроме того, предоставляется возможность работы с ведущими средствами разработки программного обеспечения, средствами управления исправлениями и информацией о безопасности.

Основные особенности Symantec Endpoint Protection

Защита от вирусов и программ-шпионов — обеспечение непревзойденной, лучшей защиты от вредоносных программ, включая ведущую защиту от вирусов, улучшенную защиту от программ-шпионов, защиту от новых угроз типа руткит, использование меньшего объема памяти и новые динамические настройки производительности для поддержания эффективности пользователей.

Защита от сетевых угроз — предоставляет модуль брандмауэра на основе правил, а также модуль Generic Exploit Blocking (GEB), который блокирует вредоносные программы до их попадания в систему.

Превентивная защита от угроз — обеспечение защиты от неизвестных угроз (т.е. угроз типа эксплойт «нулевого дня»). Включает модуль превентивного поиска угроз Proactive Threat Scan, который не основывается на сигнатурах.

Единый агент и единая консоль управления — обеспечивает управление защитой от вирусов и программ-шпионов, брандмауэром настольного компьютера, технологиями IPS, устройствами и доступом к сети (при приобретении лицензии Symantec Network Access Control) на едином агенте. При этом, все управление осуществляется с единой консоли.

Все клиентские машины работают на Windows 7 Enterprise — это выпуск Windows 7, в котором реализованы уникальные технологии, ориентированные на нужды корпоративных клиентов. Windows 7 Enterprise доступна исключительно клиентам, купившим Software Assurance для операционной системы. Помимо функций Windows 7 Professional, заказчики Windows 7 Enterprise получают дополнительные инструменты призванные обеспечить пользователю плодотворную работу в офисе и за его пределами, улучшить безопасность, повысить контроль и сделать администрирование ПК более простым и гибким.[26]

Все клиентские машины объединены в домен Active Directory. С помощью Active Directory заказчики могут управлять удостоверениями и взаимоотношениями, формирующими сеть организации. Службы Active Directory интегрированы с Windows Server 2008 R2, могут использоваться сразу после развертывания и позволяют организациям централизованно настраивать параметры систем, пользователей и приложений и управлять этими параметрами. Доменные службы Active Directory (AD DS) хранят данные каталогов и управляют взаимодействием между пользователями и доменами, в том числе входом в домен, проверкой подлинности и поиском в каталоге. Кроме того, интегрированные роли поддерживают средства и технологии управления удостоверениями и доступом, которые позволяют централизованно управлять технологиями и учетными данными и предоставлять доступ к устройствам, приложениям и данным только уполномоченным пользователям. Бронирование номеров производится системой управления гостиницей epitome PMS от компании «Libra Hospitality». Компания «Libra Hospitality» представляет новый функционал проверенной временем системы управления гостиницей epitome PMS. Пользователи сразу почувствуют разницу, работать станет еще удобней, так как оптимизирован размер рабочей области. Доработано основное окно карточки гостя, для удобства пользователей активное поле выделяется «цветом», также некоторые поля, ранее требовавшие заполнения вручную, заменены на ниспадающие списки. Глобально переработан модуль «Горничных». Новый функционал модуля позволяет максимально гибко управлять видами уборок номерного фонда, а также стало удобнее осуществлять контроль над работой горничных. Добавлен дополнительный вид пользователей — «техник». При назначении заданий на ремонт конкретному сотруднику есть возможность контролировать срок исполнения, а с помощью функция досрочного выполнения, Вы сможете видеть, кем и когда выполнено задание. Теперь в системе можно вести контроль за состоянием служебных помещений. При необходимости можно настроить служебные помещения и назначать по ним задания на уборку. По умолчанию после ночного аудита служебные помещения переходят в статус «грязный». На основное окно экрана бронирования выведено время заезда и выезда, данная информация дополнительно отображается в диаграмме и таблице наличия комнат, таким образом, теперь есть возможность просматривать наличие номеров на определенное время. В дополнительных функциях счета гостя (Folio tools- Инструменты фолианта) появилась возможность заранее и единовременно начислять всю стоимость услуги проживания и пакета, при этом во время ночного аудита система не будет начислять тариф повторно. Теперь Folio tools (Инструменты фолианта) позволяет разделять уже начисленную на счет транзакцию, а также автоматически рассчитывать почасовую оплату, либо по текущему тарифу гостя, либо по специальному тарифу, в зависимости от настроек гостиницы. Добавлена возможность фиксировать всех дополнительных гостей, которые проживают совместно с гостем и не платят за себя. Разработан и успешно внедрен новый интерфейс с популярной системой он-лайн бронирования «TravelLine», которую используют более 200 гостиниц в России. При использовании этого интерфейса все брони с сайта гостиницы автоматически попадают в epitome PMS (Property management system — Система управления гостиницей) без участия оператора.

Для финансовой отчетности используется программа «Астрал Отчет» и СБиС++ версии 1.9. В комплексе СБиС++ версии 1.9 предусмотрен целый ряд возможностей. С одной стороны программа доступна широкому кругу пользователей с самыми разными запросами, а с другой — для каждого пользователя имеющиеся возможности делают работу максимально комфортной и эффективной: удобный интерфейс, минимальные системные требования, многопользовательская работа, принцип работы от первичного документа, правила типовых операций, гибкая настройка программы под конкретного пользователя, разграничение прав доступа к информации, доступ к данным и обмен информацией с другими программами. Современное программное обеспечение «Астрал Отчет» является доступным, простым в использовании решением, позволяющим безопасно и оперативно передавать конфиденциальные данные посредством глобальной сети Интернет. Отправка отчетности в контролирующие органы без необходимости личного посещения учреждений, возможность отправки данных в Федеральную Налоговую Службу, Пенсионный Фонд России, Росстат, Фонд Социального Страхования. Отчетность для налоговой без бумажной волокиты. Быстрая отправка электронной формы по защищенным шифрованием каналам передачи данных, система электронной подписи, подтверждающая юридическую силу документов, что позволяет исключить необходимость дублирования отчетов на бумажных носителях. Круглосуточная отправка отчетности. Теперь нет необходимости тратить драгоценное время на поездки в контролирующие органы — отчетность можно отправить в считанные секунды, в любое время суток. Надежная система шифрования данных, соответствующая стандартам, принятым действующим законодательством, защита информации от несанкционированного доступа. Простота использования программного решения, нет необходимости в дополнительном обучении, удобство установки и запуска приложения без посторонней помощи. Для начала работы с системой «Астрал Отчет» нет необходимости назначать выезд технического специалиста. Возможность автоматического обновления компонентов программного решения. Обновление форм подготовки отчетности происходит автоматически при запуске программы. Взаимодействие с модулями «1С», возможность импорта отчетности из бухгалтерских приложений, автоматический контроль правильности заполнения формы отчетности. Вся передаваемая информация имеет юридическую силу, благодаря использованию электронной подписи.

Программы имеют встроенные криптографические (Приложение 3) модули Криптопро — линейка криптографических утилит (вспомогательных программ) — так называемых криптопровайдеров. Они используются во многих программах российских разработчиков для генерации электронной цифровой подписи, работы с сертификатами и т.д.

Все клиентских машин защищены шифрованием диска BitLocker Drive Encryption — проприетарная технология, являющаяся частью операционных систем Microsoft Windows Vista Ultimate/Enterprise, Windows 7Ultimate/Enterprise и Windows Server 2008 R2. BitLocker позволяет защищать данные путём полного шифрования диска(ов) (логических, с Windows 7 — и карт Secure Digital Memory Card (CD) и Universal Serial Bus (USB) -флешек) (в терминологии Microsoft — тома(ов)). Сам ключ может храниться в Trusted Platform Module (TPM Модуль платформы, которому доверяют) или в Universal Serial Bus (универсальная последовательная шина) — устройстве. Либо же в компьютере. В случае с TPM при загрузке компьютера ключ может быть получен из него сразу, либо только после аутентификации с помощью USB-ключа или ввода PIN-кода пользователем.

Сам вид деятельности гостиничного комплекса «Калуга Плаза» требует в работе особо строго соблюдения закона о защите персональных данных. Для этих целей было закуплено сертифицированное лицензионное программное обеспечение и различные криптографические средства защиты.

Калуга плаза делает упор только на лицензированное Федеральный закон и сертифицированное [19] программное обеспечение и программно-аппаратный комплекс так как только они могут обеспечить должный уровень безопасности гостиницы. Руководство гостиницы придерживается информационной безопасности и поэтому со всеми сотрудниками подписывается договор о неразглашении коммерческой тайны и конфиденциальной информации. Со всем персоналом постоянно проводятся тренинги и семинары на тему коммерческой тайны и конфиденциальной информации. Для этих целей приглашаются специалисты администрации комплекса, а также сторонние специалисты.   .5 Анализ системы доступа в помещения гостиницы

Современная гостиница, это объект, где обеспечение безопасности играет ключевую роль. Как правило, это здание с большим количеством комнат и длинных коридоров, оживленное и днем и ночью фойе и приемная, увеселительные учреждения на первом этаже. Ежедневно приезжают туристы из различных городов и стран, останавливаются работники самых различных фирм из разных городов во время рабочих командировок. У всех имеются с собой вещи, ценные предметы и, конечно же, денежные средства. Все эти обстоятельства притягивают большое количество мошенников и воров, желающих поживиться чужим имуществом, и просто преступников, для которых гостиница является местом, где можно затеряться среди большого числа людей. Конечно, в серьезных гостиницах имеется служба безопасности, но одного лишь профессионализма ее работников уже недостаточно для того, чтобы держать ситуацию под контролем — и здесь на помощь приходят современные технические средства.

Установка системы электронных замков еще одно из самых эффективных профилактических средств повышения безопасности. По некоторым оценкам, внедрение системы электронных замков позволяет снизить уровень краж на 95%. Практически невозможна подделка конкретного ключа, а также можно определить, какими карточками был открыт номер, в какое время и кто их выдал.

Руководство гостиничного комплекса «Калуга Плаза» очень серьезно отнеслось к решению этой проблемы. Вопросы оборудования гостиничных предприятий электронными системами безопасности особо важны для небольших гостиниц, где ограничено количество персонала. Поэтому номерные фонды гостиничного комплекса «Калуга Плаза» оснащены электронными замками Classic by VingCard фирмы « Norweq»[38]. Руководство выбрало такой тип защиты потому, что современные технологии и высококачественные материалы позволяют VingCard гарантировать работоспособность замков в тяжёлых, подчас экстремальных условиях. Например, при испытании механизма подтяжки ручки количество открываний достигло отметки в 1200000 раз без видимых следов износа, исключительная надежность (проверенная временем), первоклассные материалы, стойкое покрытие панели, использование профессиональных электромеханических корпусов замков, устойчивое и богатое функциональное программное обеспечение, надежное периферийное оборудование для гостиниц любого уровня, предпочитающих классический стиль и надежность.

·  лёгкая установка

·        перепрограммируемая флэш-память

·        магнитная полоса, смарт-чип или комбо (магнитная полоса + смарт-чип)

·        системы управления 2800 или VISION

·        600 событий в энергонезависимой памяти

·        В отчётах доступны ФИО как сотрудников, так и гостей

·        3 режима работы: режим гостевого номера, офисный режим (режим «свободного прохода») и автоматическое переключение между этими режимами

·        технология RealTime — технологии реального времени, т.е. возможно отложенное поселение, а на каждой карточке есть «временное окно» в течение которого эта карточка действительна

·        направление движения карточки — горизонтально вперед-назад

·        противопожарный тест UL (3 часа)

·        электромагнитный тест ЕМС

·        двойное считывание карточки для надёжности

·        ADB Plus (AutoDeadbolt Plus) — автоматический выход ригеля в дополнение к фиксирующейся защёлке (опция)

·        питание — 4,5В (3хАА)

·        элементы питания во внутренней части замка (внутри номера)

·        профессиональный электромеханический корпус замка

·        не требует смазки и/или иного технического обслуживания кроме чистки головок

·        крепеж замков имеет нестандартную конфигурацию головки

·        закалённый ригель, защёлка состоит из 3-х частей

·        функция «Анти-паника» — свободный выход из номера

·        функция «Не беспокоить» — поворотная кнопка изнутри, работает также при использовании ADB Plus

·        корпуса замков EURO 22-24-25 или ANSI 25-28-32

·        ручки — Standard Scandinavia, Ship, US Ship, Wing, Straight, ANSI 1, Functional ANSI, Functional EURO, Gothic, Special 45, Flair, Knob, High Tech. Все ручки изготовлены из цельнолитой латуни или алюминия (Престо). Специальные ручки изготавливаются под заказ (Russian)

·        отсутствие винтов крепления ручек снаружи и внутри

·        цилиндр — высокосекретный, перепрограммируемый, 3 или 5 уровней (опция)

·        накладки — плоские или в готическом стиле. Каждая накладка состоит из двух частей: внутренняя часть — пластина из стали холодного проката для защиты корпуса замка, внешняя часть из латуни в отделке по вашему выбору.

·        отделки: полированный и неполированный хром, полированная и неполированная латунь, светлая бронза, цвета по таблице RAL, Velour Nickel.

·        специальная отделка для агрессивных сред (например, для установки на внешних дверях коттеджей) — анодированный алюминий. Варианты — под серебро, под золото, коричневый. Ручка — Престо. 7 лет заводской гарантии

Дополнительные опции:

·        крышка от осадков

·        влагозащитная прокладка

·        залитые компаундом элементы питания

·        цельнометаллическое исполнение (All Metal) — все внешние пластиковые элементы выполнены в металле

Для использования таких замков применяются пластиковые карточки с магнитной полосой. Для их кодирования используется сетевой многодорожечный энкодер — многодорожечный энкодер записывает информацию на все три дорожки магнитной полосы. Таким образом, например, сигнал посланный из АСУ Гостиница может быть записан на вторую дорожку для использования в системе безналичных расчётов гостиницы. Обычно это — бары, рестораны, магазины и другие точки продаж внутри гостиничного комплекса. Для программирования электронных замков используется сервисное устройство ЛокЛинк (LockLink) выполненного на базе карманного компьютера (КПК) с операционной системой Windows Mobile. С помощью ЛокЛинка производится первоначальное программирование и последующее перепрограммирование замков, считывание с них информации (600 событий), а также экстренное открывание замка (при отсутствии цилиндра). Устройства от НР используются потому что они одновременно надёжные и доступные. В состав ЛокЛинка входит собственно сам КПК (Карманный Персональный Компьютер), инфракрасный порт для соединения с замками и другими устройствами и программное обеспечение. Таким образом, при потере или поломке сервисного устройства, гостиница не привязана к поставщику замков, а может приобрести КПК в любом компьютерном магазине.

Для остальных помещения гостиничного комплекса «Калуга Плаза» используются обычные механически замки. Ключи от них находятся у службы безопасности под личным контролем.

Вывод

. Внешние лица имеют меньше возможностей доступа к ресурсам безопасности системы гостиничного комплекса «Калуга Плаза», чем внутренние пользователи, и представляют из себя меньшую угрозу. В то же время, на них очень сложно или почти невозможно влиять, поэтому для эффективной защиты от внешних угроз гостиничного комплекса «Калуга Плаза» необходимо в первую очередь использовать внутренние технические и организационные меры.

. Безопасность гостиничного комплекса «Калуга Плаза» разделена на несколько уровней доступа. Сотрудник получает доступ только к тем сведениям и производственным мощностям, которые необходимы ему для работы. Необходимо утвердить список доступа в гостиничном комплексе, отнесенной к разряду комплексной безопасности, сотрудники должны быть ознакомлены с ним под роспись. Доступ к конфиденциальной информации возможен только после внесения сотрудника в соответствующий список, утверждаемый руководством. При принятии решения о предоставлении доступа к какой либо информации целесообразно учитывать психологические особенности и компетентность сотрудника.

. Желательно, чтобы выполнение требований безопасности рассматривалось в качестве одного из критериев оценки работы, и нарушение этих требований должно приводить к наказанию, определенному внутренними нормативными документами. Наряду с рядовыми сотрудниками ответственность за соблюдение правил безопасности должны нести менеджеры и инженеры-технологи. Выполнение внутренних регулирующих документов в части, касающейся информационной безопасности, должно контролироваться службой информационной безопасности гостиничного комплекса «Калуга Плаза». При этом сотрудникам необходимо объяснить, что контролируются не люди, а производственные процессы, и что такой контроль соответствует их личным интересам, так как защищает от давления на них и близких им людей со стороны криминальных структур.  
3 .Система безопасности гостиничного комплекса   .1 Организационные меры по безопасности гостиничного комплекса

При организации системы безопасности в гостинице необходимо четко представлять себе, для каких целей и за счет каких средств она будет функционировать. Случается, что при решении вопроса безопасности руководители гостиницы впадают в две крайности или они тратят значительные средства на организацию суперсложных систем безопасности, применяющихся на объектах повышенной секретности, или же доверяют решение этой проблемы «умельцам», обещающим «за копейки» организовать систему безопасности, отвечающую мировым стандартам. Главная задача разработки концепции безопасности реализация условий, при которых клиенты гостиницы и ее сотрудники могли бы чувствовать себя уверенно, спокойно и комфортно.

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.

В процессе концептуального проектирования проводится:

·        формирование вариантов построения комплекса инженерно-технических средств системы безопасности (ИТССБ);

·        формирование вариантов оснащения охраняемых зон, обоснование выбора ИТССБ;

·        формирование предложений по защите информации в системе безопасности;

·        формирование предложений по использованию персонала безопасности;

·        формирование предложений по организационным мероприятиям;

·        оценка эффективности и стоимости предлагаемого (предлагаемых) варианта построения ИТССБ.

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.

Комплекс (от лат. Complex — связь, сочетание) — система, совокупность чего-либо.

Система (от др. греч. σύστημα — целое, составленное из частей; соединение) — множество элементов, находящихся в отношениях и связях друг с другом, которое образует определённую целостность, единство. В любой системе можно выделить отдельные части, выполняющие некоторые функции и взаимодействующие друг с другом.

Работа персонала гостиницы предполагает индивидуальный подход к каждому посетителю. А в сфере безопасности ключевое значение приобретает правильный выбор технических средств, оптимальное проектирование систем, их монтаж и обслуживание.

Служба безопасности предусматривает следующий комплекс организационных мероприятий:

·        Организация контрольно-пропускного и транспортного режима;

·        Обеспечение безопасности клиентов гостиницы и сохранности их имущества;

·        Обеспечение личной безопасности штатных работников на рабочем месте;

·        Пресечение различных антиобщественных проявлений и поддержание общественного порядка в здании объекта и на прилегающей к нему территории;

·        Организация патрулирования охраняемой территории;

·        Контроль работы систем охраны, жизнеобеспечения и коммуникаций (систем видеонаблюдения, контроля и управления доступом, пожарной и охранной сигнализации);

·        Контроль парковочной зоны, охрана транспортных средств посетителей и сотрудников персонала.

Технические средства являются основой системы безопасности гостиницы по нескольким причинам. Во-первых, техника не подвержена усталости, невнимательности, болезням, сиюминутным чувствам, погодным условиям. Во-вторых, к ней неприменим подкуп, шантаж и запугивание, и неспециалисту сложно ее обмануть. Ну и, в-третьих, в ней изначально предусмотрены мгновенная реакция и точность выполнения заданных алгоритмов. Однако эти преимущества должны в обязательном порядке дополняться возможностями сотрудников службы безопасности. Только тесное взаимодействие специалистов и техники способно обеспечить оперативное реагирование на тревожную ситуацию и комплексно разрешить возникающие проблемы.

Основные работы для организации мер по безопасности гостиничного комплекса:

·        проектирование, монтаж интегрированной системы безопасности, вентиляции, кондиционирования, отопления, энергообеспечения;

·        автоматизация и диспетчеризация всех внутренних инженерных систем, централизацию наблюдения и контроля над удаленными объектами;

·        многоуровневую архитектуру и разграничение прав доступа к информации;

·        взаимодействие систем безопасности и жизнеобеспечения;

·        интеллектуальный анализ информации;

·        автоматизацию производственных циклов;

·        технический мониторинг инженерных систем;

·        распознавание и автоматический учет подвижных объектов;

·        передачу информации по оптоволоконной линии порта и по сети Wi-Fi.  
3.2 Угрозы безопасности гостиничного комплекса

Наличие технических средств безопасности в современном отеле является обязательным условием ее успешного функционирования. Предоставление гарантий безопасности — показатель определенного качества обслуживания, фактор привлечения клиентов и возможность обретения их лояльности в дальнейшем.

В гостинице постоянно присутствует движение людских потоков и материальных ресурсов, что требует предельной концентрации и внимания персонала. Большое скопление людей и поток туристов делают гостиницы привлекательным местом для различных криминальных элементов, желающих остаться незамеченными.

Выделим основные источники угрозы:

·        пожар, причинами которого могут быть небрежность гостей, неисправность электрооборудования, несоблюдение или нарушение правил противопожарной безопасности, умышленный поджог;

·        взрыв вследствие утечки газа или организованный в криминальных/террористических целях;

·        несанкционированный проход посторонних лиц в номера с целью кражи материальных ценностей и документов постояльцев, установки взрывных устройств или подслушивающей аппаратуры;

·        несанкционированный проход в номера обсуживающего персонала с теми же криминальными целями;

·        нападение на гостей в номерах, лифтах, других помещениях гостиницы;

·        ограбление кассы в рабочее время, попытка ее вскрытия в нерабочее время;

·        кража имущества гостиницы персоналом;

Перечень возможных мест повышенного интереса криминальных групп:

|  |  |
| --- | --- |
| Места повышенного интереса | Возможная акция |
| Касса | Вооруженное ограбление |
| Камера временного хранения ценностей | Вооруженное ограбление, кража |
| Зал приема/оформления гостей и место хранения ключей | Захват заложников, хищение ключей |
| Помещения высшей администрации | Захват заложников, вооруженное нападение, убийство |
| Помещения службы безопасности | Нейтрализация охраны и системы сигнализации |
| Гостиничные номера и особенно апартаменты люкс | Ограбление, кража, нападение на гостей |
| Помещения для конфиденциальных переговоров | Установка подслушивающей аппаратуры |
| Ресторан | Вооруженное ограбление, захват заложников |

3.3 Технические средства безопасности гостиничного комплекса

Для отелей с развитой инфраструктурой (конференц-залом, магазинами, ресторанами, казино, парковкой и проч.) установленные видеокамеры и считыватели карт доступа — оптимальный способ защиты гостей, персонала и имущества. Организация централизованного поста наблюдения для сотрудников службы безопасности, запись и хранение полученной информации с видеокамер и считывателей за продолжительное время позволяют быстро выявлять участников и пресекать возможные правонарушения, создавая максимальный комфорт для постояльцев.

Интеграция всех инженерных систем и систем безопасности гостиницы в единый комплекс с возможностью одновременного вывода информации о состоянии систем является незаменимым источником информации о текущей ситуации на объекте для службы безопасности, руководства или владельцев гостиницы. Одновременно можно осуществлять контроль работы обслуживающего персонала и повышать уровень качества обслуживания постояльцев.

Интегрированная система безопасности гостиничного комплекса, как правило, включает в себя несколько отдельных систем — систему контроля и управления доступом (СКУД), видеонаблюдение (CCTV), охранную и пожарную сигнализации (ОПС).

В зависимости от комплекса и прилегающей территории в него могут также входить система охраны периметра, активного пожаротушения, инженерно-технические системы обеспечения жизнедеятельности здания (лифты, вентиляция и кондиционирование) и проч. Каждая из этих систем отвечает за свой участок работы в соответствии с задачами, которые были заложены в нее на этапе проектирования.

Система контроля и управления доступом (СКУД)

Конфигурация системы и количество оборудования зависят от размеров гостиничного комплекса, объема номерного фонда и решаемых задач. Основное назначение любой СКУД — контроль и управление процессом доступа людей, транспорта и других объектов в здания, отдельные помещения (группы помещений) и территории. Контроллеры объединены в единую информационную сеть программным обеспечением. Как правило, на базе СКУД строится Интегрированный комплекс безопасности всего объекта, поскольку данная система обладает наиболее мощной и развитой встроенной логикой. Данная подсистема непосредственно связана с компьютерными терминалами управления.

Основные функции СКУД:

управление процессом доступа в соответствии с заранее присвоенными полномочиями,

регистрация факта входа/выхода с привязкой ко времени,

возможность управления процессом доступа в каждое помещение,

автоматизация однообразных процессов.

предотвращение заселения номеров без регистрации,

автоматическое предоставление доступа гостям в номера и другие помещения по электронным ключам (картам доступа),

контроль действий персонала, управление доступом сотрудников в помещения, учет рабочего времени,

автоматизация ограничения доступа в номера по времени (заселения и выселения),

превышение времени проживания в гостинице,

формирование различных отчетов (о времени пребывания в номере сотрудников, маршрутах горничных и т.п.),

автоматическое управление освещением в номерах (автоматическое выключение и включение света при уходе и приходе гостя),

контроль доступа на автопарковку,

организация рабочих мест отдела кадров/службы безопасности/стойки регистрации гостей.

Для защиты от не санкционированного доступа в номерные фонды предлагаю использовать электронные замки VingCard.

Современные технологии и высококачественные материалы позволяют VingCard гарантировать работоспособность замков в тяжёлых, подчас экстремальных условиях.

К числу некоторых уникальных возможностей VingCard можно отнести:

исключительная надёжность, проверенная временем

первоклассные материалы, например, цельно-литые латунные ручки

стойкое покрытие панелей

использование профессиональных электромеханических корпусов замков

устойчивое и богатое функционально программное обеспечение

надёжное периферийное оборудование

Гостиничные электронные замки имеют свои особенности, это не только замок, но и система безопасности, и элемент декора гостиницы; система электронных замков ещё и часть технологического процесса обслуживания Гостя.

Видеонаблюдение.

Система видеонаблюдения на территории гостиничного комплекса необходима для обеспечения визуального контроля над обстановкой, анализа возможных внештатных ситуаций, проверки истинности поступающих сигналов тревоги, помощи в принятии оперативных решений. Только система видеонаблюдения может помочь отследить и зафиксировать каждый произошедший инцидент, идентифицировать мошенника или поймать за руку нечестного сотрудника.

Основные решаемые задачи на территории гостиничного комплекса с помощью системы видеонаблюдения:

·        круглосуточное наблюдение за территорией комплекса,

·        периметральное видеонаблюдение,

·        контроль ситуации в холлах и служебных помещениях,

·        включение видеокамер для записи при заданном событии,

·        регистрация проходящих через пост охраны отдыхающих и сотрудников гостиницы,

·        распознавание и регистрация номеров автотранспорта,

·        запись, просмотр и поиск видеоархива и т.д.

Необходима установка видео камер в таких наиболее уязвимых с точки зрения обеспечения безопасности участках отеля, как:

·        зона входа в гостиницу, территория автомобильной стоянки;

·        стойка приема и оформления гостей, место хранения ключей;

·        фойе и расположенные на первом этаже предприятия питания и магазины;

·        коридоры, лестничные пролеты, эвакуационные лестницы, часто использующиеся персоналом.

В Интегрированном комплексе безопасности система видеонаблюдения существенно повышает свою эффективность, поскольку становится возможным активирование камер CCTV по событиям в других подсистемах. Примером может служить ситуация, когда человек заходит в здание/помещение, приложив карту к считывателю, на мониторе у охранника одновременно выводится фотография из базы данных и транслируется изображение с видеокамеры в реальном времени, — что позволяет осуществить удаленный визуальный контроль и принять решение о праве доступа.

Программное обеспечение позволяет вести точный учет находящихся на территории людей, иметь видеоархив лиц людей, прошедших через пост охраны, также будет доступна отчетность о количестве автомобилей отдыхающих и сотрудников, времени их нахождения на территории.

Для контроля видеонаблюдения можно предложить использование видеокамер VJR-F801-ICCV для установки внутри помещения и камеры EX85 для наружной установки по периметру.

Система охранно-пожарной сигнализации

Основные решаемые задачи на территории гостиничного комплекса с помощью системы охранно-пожарной сигнализации:

·        противопожарная безопасность в номерах, холлах и служебных помещениях,

·        охранная и тревожная сигнализация,

·        автоматическое включение/выключение кондиционера, системы вентиляции при достижении в помещении определенной температуры или влажности, а также при выходе постояльца из номера;

·        автоматическая/ручная постановка и снятие с охраны номера, служебного помещения при уходе и приходе сотрудника или гостя.

Гостиничный комплекс должен быть оборудован пожарной сигнализацией и средствами пожаротушения, обеспечивающими эффективное обнаружение очага возгорания. По всем помещениям монтируются дымовые датчики и устанавливается автоматическая система пожаротушения. Каждый гостиничный номер желательно обеспечить индивидуальными средствами защиты, а планировка здания должна соответствовать требованиям, позволяющим своевременно и оперативно эвакуировать людей даже из высотных зданий. Для предотвращения паники при эвакуации в отеле устанавливается система голосового оповещения.

Интегрированный комплекс безопасности.

В любом гостиничном комплексе постоянно идет усложнение процесса управления, ставятся новые задачи, увеличивается число управляющих устройств и, соответственно, растет нагрузка на службу безопасности. При этом часть наиболее трудоемких функций в этой области можно и нужно передавать электронной системе безопасности, чтобы сократить воздействие «человеческого фактора» и, как следствие, финансовые потери. Современные ИКБ представляют собой аппаратно-программные комплексы с общей базой данных. В качестве устройств управления используются компьютеры со специализированным программным обеспечением. Главенствующую роль в ИКБ выполняет СКУД, поскольку обладает наиболее мощной и развитой встроенной логикой. Интегрированный комплекс безопасности должен объединять подсистемы так, чтобы их узкая направленность не приводила к противоречиям при разрешении конкретных ситуаций на объекте.

Интеграция всех подсистем в единую систему позволяет реализовать в гостиничном бизнесе следующие функции:

·    разграничить полномочия, регистрацию и документирование проходов постояльцев и персонала в номера и служебные помещения;

·        разделить постановку и снятие с охраны каждого номера (в том числе и автоматически по чтению электронной карты);

·        оперативно вмешаться в работу системы и целевое управление каждым из ее узлов (включить/выключить вентиляцию, открыть/заблокировать дверь, аннулировать право прохода и проч.);

·        установить дистанционный видеоконтроль и видеорегистрацию событий;

·        оперативно получать различные отчеты по заданным параметрам фильтрации;

·        возможность удаленно управлять инженерными коммуникациями в здании (лифты, свет, кондиционирование и проч.).

Интеграция в систему управления гостиничным комплексом.

Отельный бизнес подразумевает наличие значительного объема работы по учету, контролю и статистической обработке информации. Для бронирования номеров предлагаю программное обеспечение Epitome PMS. Система управления гостиницей Epitome PMS для платформы Microsoft® Windows — это новейшее поколение систем автоматизации компании Softbrands Inc., входящих в семейство программных продуктов epitome Solutions. Система epitome PMS сертифицирована Microsoft, проста в использовании и обладает необходимой гибкостью для применения в управлении гостиницами любого типа, категории и размера. Мощный функциональный инструментарий Epitome PMS позволит создать успешную технологию ведения бизнеса гостиницы, повысить финансовые показатели и достичь высокого уровня сервиса для гостей.PMS построена по модульному принципу, что позволяет гостиницам приобретать и настраивать систему в соответствии со своими потребностями. В зависимости от набора модулей система успешно функционирует как в небольших гостиницах, так и в крупных гостиничных комплексах и цепочках. Модули системы разработаны в едином техническом и технологическом стиле и имеют общий функциональный инструментарий и взаимосвязь.

Основываясь на наиболее передовых технологиях, система управления гостиницей Epitome PMS функционирует в среде Windows, обладает 32-битной архитектурой и открытой структурой данных под управлением мощной СУБД MS SQL Server. Epitome PMS имеет несколько встроенных модулей из которых хотелось бы выделить паспортный модуль для бронирования и регистрации иностранных граждан которые имеют возможность в автономном режиме отсылать регистрационные данные в органы УФМС.

Вывод

Таким образом, основная сложность при разработке системы безопасности гостиницы связана с хаотичными перемещениями большого количества посетителей. Электронные системы открывают дополнительные возможности. Во-первых, легко предотвращаются попытки так называемых «левых поселений», ведь администрация всегда сможет проверить правомерность использования того или иного электронного ключа. Сколько денег теряет гостиница от этих нарушений — может определить лишь руководство. По оценкам специалистов, эта цифра колеблется в пределах от 5 до 20%. Причем, чем больше гостиница, тем больше процент потерь и тем сложнее контролировать отель без специальной техники.

Во-вторых, будут предотвращены возможности кражи из номеров; повысится дисциплина, и сотрудники не будут смотреть телевизор в номере; не будет телефонных звонков из незаселенного номера; можно сэкономить на персонале, так как после установки подобных систем отпадает необходимость в поэтажных дежурных, выдававших ранее ключи и многое другое. Заключение

В данной выпускной квалификационной работы рассмотрена система безопасности гостиничного комплекса. Изложены основные сведения, которые требуются для организации данной защиты, а также были разработаны, в соответствии с основными требованиями и ГОСТами, система безопасности гостиничного комплекса.

Поставленные задачи исследования выполнены в полном объеме:

·        представлены с позиции системного подхода требования к системе безопасности гостиничного комплекса;

·        выбраны и обоснованы методы и средства системы безопасности гостиничного комплекса;

·        выполнена оценка типовой системы по эффективному показателю прочности построенной защиты.

В ходе сбора материала для выпускной квалификационной работы, анализа литературных источников и собственных наблюдений сделаны следующие выводы:

·        учитывая многообразие потенциальных угроз системе безопасности, сложность их структуры и функций, а также участие человека в процессе разработки системы безопасности, цели системы безопасности могут быть достигнуты только путем создания системы безопасности на основе комплексного подхода;

·        основным требованием к системе безопасности на момент её построения является отсутствие уязвимостей или сведение их к минимальному риску;

·        создание системы безопасности является непрерывным процессом, поддержание ее в актуальном состоянии является прямой обязанностью ответственных специалистов.

Разработка системы безопасности гостиничного комплекса должна представлять собой целостную систему защитных мероприятий таких как:

Предложения (рекомендации) для зоны высшего руководства гостиничного комплекса сводятся к применению комплекса защитных мероприятий:

·        создание рубежной защиты с разделением зон по источникам возможных угроз для системы безопасности.

·        применение сертифицированных средств защиты.

·        относиться серьезно и профессионально к организации кадровой политики, так как на ней и начинается обеспечение дальнейшей информационной безопасности в плане подборки персонала гостиничного комплекса;

·        проводить постоянные исследования в области информационных технологий на наличие некачественного обеспечения безопасности электронной документации и программ их хранения. А также новых технологий позволяющих существенно улучшить систему обеспечения безопасности в ЭВМ;

·        периодически вырабатывать новые принципы системы контроля и управления доступом, дабы обезопасить гостиничный комплекс, со стороны нарушения персонала, который может воспользоваться недоработанными старыми методами, для хищения информации;

·        обращать тщательное внимание на изменения правовой базы.

Они не возможны без применения широкого спектра защитных средств, объединенных в единую архитектуру. Далеко не все эти средства получили распространение в России, некоторые из них даже в мировом масштабе в стадии становления. Разумеется, представленный вариант системы защиты это не полный перечень, поскольку каждый руководитель решает какие методы и средства защиты необходимо использовать применительно к данному объекту, что зависит от функций, выполняемых объектом, а также от его экономических соображений. Таким образом, главная цель данного исследования была достигнута, произошло определение требований к системе безопасности для зоны высшего руководства гостиничного комплекса и обоснование применимых технических средств.

Большое внимание в исследовании уделено способам защиты информации представляемой в электронном виде. Рассмотренные средства защиты электронной информации базируются на основе трех составляющих:

·        разграничения доступа к защищаемым ресурсам;

·        криптографического закрытия защищаемой информации;

·        методы противодействия утечкам происходящих за счет побочных электромагнитных излучений и наводок.

В результате выполнения поставленных задач была разработана типовая система безопасности гостиничного комплекса для зоны высшего руководства промышленного предприятия.

ВКР может иметь теоретическую и практическую значимость, прежде всего как сбор материала на рассматриваемую тему, под определенным углом зрения, а именно: разработка системы безопасности гостиничного комплекса, реализованная для предотвращения угроз объекту защиты.

В последующем данная система безопасности может быть легко модифицирована под архитектуру нового поколения на основе Ethernet. Данные системы отличаются от традиционных, что вся взаимосвязь блоков устройств работает за протоколом Ethernet. Их создание стало возможным благодаря появлению необходимых мощных микроконтроллеров и IP- камер. Работа всех устройств системы по одному и тому же протоколу, в одной и той же сети обуславливает на порядок более высокую надежность и позволяет привлекать для обслуживания уже имеющихся IT- специалистов.

В этих условиях позиция по отношению к системе безопасности должна быть особенно динамичной. Теоретические воззрения, стандарты, сложившиеся порядки необходимо постоянно сверять с требованиями практики. От угроз не защитится законами и сертификатами, они будут применимы в ходе последующего расследования инцидента, а ценная информация будет потеряна. Реальная безопасность нуждается в каждодневной работе всех заинтересованных сторон.

Поставленные задачи решены, цель достигнута.  
Библиографический список

1. Гражданский кодекс РФ 2012 (с изменениями и дополнениями)

2. Федеральный закон Российской Федерации «О безопасности» от 09.02.2007 г. №390-ФЗ (ред. от 28.12.2010 г.)

3.       Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями от 27 июля 2010 г., 6 апреля, 21 июля 2011 г.)

4. Федеральным законом «О пожарной безопасности» от 21.12.94 № 69-ФЗ (ред. от 30.11.2011)

5.       Федеральный закон «Об основах туристской деятельности в РФ» от 24.11.1996 №132-ФЗ (в ред. Федеральных законов от 10.01.2003 N 15-ФЗ,от 22.08.2004 N 122-ФЗ, от 05.02.2007 N 12-ФЗ,от 30.12.2008 N 309-ФЗ, от 28.06.2009 N 123-ФЗ,от 27.12.2009 N 365-ФЗ, от 30.07.2010 N 242-ФЗ,от 01.07.2011 N 169-ФЗ)

6.       Федеральный закон «О коммерческой тайне» от 29.07.2004 г. (в ред. от 11.07.2011 г.)

7.       ТК 199 “Туристические услуги и услуги средств размещения”. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 773-ст. Взамен ГОСТ Р 50644-94. Постановление Правительства РСФСР от 05.12.91 № 35 «О перечне сведений, которые не могут составлять коммерческую тайну»

8. Международный стандарт ISO/IEC 15408 «Информационная технология — методы защиты — критерии оценки информационной безопасности»

9.       Международный стандарт ISO/IEC 17799 «Управление информационной безопасностью»

10.     ГОСТ Р 50644-2009 от 15.12.2009 «Требования по обеспечению безопасности туристов и экскурсантов» Разработан Открытым акционерным обществом “Всероссийский научно-исследовательский институт сертификации”, Департаментом туристской деятельности и международного сотрудничества Министерства спорта, туризма и молодежной политики Российской Федерации с участием Федерального агентства по туризму. Внесен Техническим комитетом по стандартизации ТК 199 “Туристические услуги и услуги средств размещения”. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 773-ст. Взамен ГОСТ Р 50644-94.

11.     ГОСТ Р 51624-00 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования». М.: Госстандарт России.

12.     ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Архитектура защиты информации». М.: Госстандарт России.

13.     ГОСТ Р 51241-99 «Технические средства защиты и охраны. Средства и системы контроля и управления доступом. Классификация, общие технические требования, методы испытаний». М.: Госстандарт России.

14.     ГОСТ Р 51558-2000 «Системы охранные телевизионные. Общие технические требования и методы испытаний». Госстандарт России,2002

15.     ГОСТ 26342-84 «Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры». М. Госстандарт России.

16.     ГОСТ Р 50776-95 «Системы тревожной сигнализации. Часть 1.Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию». М.: Госстандарт России.(с изменениями от 12.09.2008)

17.     ППБ 01-03 (Правила пожарной безопасности) от 18.06.2003 г. №313

18.     РД78.36.003-2002 «Руководящий документ. Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств». ГУВО МВД России,2002.

19.     «Положение о сертификации средств защиты информации», утвержденное постановлением Правительства Российской Федерации от 08.08.2001 № 128-ФЗ «О сертификации средств защиты информации»№ 327-ФЗ от 21.11.2011

20.     «Положение о государственной системе защиты информации от ИТР и от утечки по техническим каналам», утвержденное постановлением Правительства РФ от 15.09.93 № 912-51

21.     «Положение о государственном лицензировании деятельности в области защиты информации», утвержденное совместным решением Гостехкомиссии и ФАПСИ при Президенте Российской Федерации от 27.04.94 №10 (с изменениями и дополнениями от 24 июня 1997 г. №60)

22.     Андрианов В. И., Соколов А. В./ под общ ред. Колесников О. В., Золотарев С. А., Шишигина И. В./ Как сберечь свои секреты.-2-е изд.-М.: ООО «Изд. ACT»;

23.     Магауенов Р.Г., Системы охранной сигнализации: основы теории и принципы построения, изд. -М.: «Горячая линия-Телеком», 2004

24.     Волхонский В.В. телевизионные системы наблюдения. Учебное пособие. СПб, Изд-во Экополис и культура,2004.

25.     Гайкович В.Н. Управление средствами защиты информации. — М.: ИНФРА-М, 2006.

26.     Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Кн. 1. — М.: Энергоатомиздат, 2007.

27.     Допира В.И., Основы безопасности предпринимательства — Тула: ТФ МАКБП, 2005.

28.     Дорошенко А.А. Инженерно техническая защита информации — Тула: ТФ МАКБ, 2008.

29.     Лаврентьев А.В. Рекомендации по организации системы защиты информации. — М.: Секьюрити, 2006.

30.     Оленин Ю.А. Основы систем безопасности объектов. Учебное пособие: Часть 1.-Пенза: Информационно издательский центр Пенз.Гос.Ун-та, 2002.

31.     Рассказов А.А. Технология защиты информации. — М.: ЮНИТИ-Дана, 2008.

32.     Технические средства защиты информации 99.-М.:ЗАО «АННА», 1999.

33.     Широчин В.П. Методика анализа и управления рисками безопасности систем. — М.: Нолидж, 2007.

34.     Ярочкин В.И. Система безопасности фирмы. — М.; Ось-89, 2004.

35.     Ярочкин В.И. Коммерческая информация фирмы. — М.; Ось-89, 1997.

36.     Ярочкин В.И. Секьюритология. — М.; Ось-89, 2000 33. Campbell R. «Economic principals, problems and politics» 14 издание перевод с английского 2002 Москва.

|  |
| --- |
| [Вернуться в библиотеку по экономике и праву: учебники, дипломы, диссертации](http://учебники.информ2000.рф/index.shtml)  [Рерайт текстов и уникализация 90 %](http://учебники.информ2000.рф/rerait-diplom.shtml)  [Написание по заказу контрольных, дипломов, диссертаций. . .](http://учебники.информ2000.рф/napisat-diplom.shtml) |

|  |  |
| --- | --- |
| [**КНИЖНЫЙ МАГАЗИН**](http://учебники.информ2000.рф/chitai.shtml) |  |

|  |  |
| --- | --- |
| [**ТОВАРЫ для ХУДОЖНИКОВ и ДИЗАЙНЕРОВ**](http://учебники.информ2000.рф/kar.shtml) |  |

|  |  |
| --- | --- |
| [**АУДИОЛЕКЦИИ**](http://учебники.информ2000.рф/lectr.shtml) |  |

|  |  |
| --- | --- |
| [**IT-специалисты: ПОВЫШЕНИЕ КВАЛИФИКАЦИИ**](http://учебники.информ2000.рф/otu.shtml) |  |

|  |  |
| --- | --- |
| [**ФИТНЕС на ДОМУ**](http://учебники.информ2000.рф/fit1.shtml) |  |