**Содержание**

Введение

1. Понятие «информационных технологий»

2. Применение информационных технологий для обеспечения безопасности клиента

2.1 Обеспечение безопасности клиента в гостинице

2.2 Обеспечение безопасности клиента в аэропорту

Заключение

Список литературы

**Введение**

Рост интереса к информационным технологиям, обеспечивающим безопасность, наблюдается во всем мире. По мнению аналитической компании ЮС, рынок межсетевых экранов, средств криптографической защиты, идентификации, авторизации, управления безопасностью, антивирусных средств имеет тенденцию к ежегодному росту 20-23%.

Информационные технологии (ИТ), являясь одним из важнейших элементов деятельности компаний, играют исключительно важную роль в обеспечении их конкурентоспособности. В этой связи становится очевидной необходимость управления эффективностью ИТ.

Как правило, затраты на информационные технологии представляют собой одну из пяти крупнейших затратных статей организаций, причем исследования показывают, что в среднем 10–25% этих затрат используется неэффективно. В современной ситуации, когда особенно остро ощущается необходимость соблюдения законодательных требований, нет ничего удивительного в том, что руководители компаний обеспокоены связанными с ИТ рисками и осознают необходимость контролировать затраты на информационные технологии (7).

Объекты (отели, аэропорты, железнодорожные вокзалы) необходимо оснастить современными системами обеспечения безопасности. Такие сложные и масштабные объекты предъявляют к системе обеспечения безопасности высокие требования по надежности, производительности, масштабируемости, функциональным возможностям. В этом случае интегрированные комплексы обеспечения безопасности вне конкуренции.

В данной работе, я хотела бы рассмотреть типовые решения по оснащению указанных объектов.

**1. Понятие «информационных технологий»**

Любые управленческие информационные процессы включают в себя процедуры регистрации, сбора, передачи, хранения, обработки, выдачи информации и принятия управленческих решений. Информационные технологии представляют собой те средства и методы, с помощью которых реализуются эти процедуры в различных информационных системах.

История развития информационных технологий может быть разбита на несколько этапов. Первый этап — это ручная технология сбора и обработки информации, господствовавшая до второй половины XIX в. Основными инструментами в то время являлись перо, чернила и простейшие счетные аппараты, а средства коммуникации были представлены в форме курьерской и почтовой связи. В конце XIX в. начался этап механической технологии. К этому времени относится создание пишущей машинки, телефона, которые существенно изменили технологию обработки информации и организационную структуру предприятий. С появлением электронных пишущих машинок, копировальных машин и диктофонов в 40—60-х гг. XX в. связывается этап электронной технологии. Массовое производство электронно-вычислительных машин в 60-х гг. и их широкое проникновение во все сферы деятельности являются началом новой компьютерной информационной технологии. Особо успешно эта технология начала внедряться с 70-х гг., когда были созданы персональные электронно-вычислительные машины.

По степени автоматизации можно выделить ручные, автоматизированные и автоматические информационные технологии. Исторически первыми были так называемые ручные информационные технологии, в которых все процедуры по сбору, обработке и передаче информации осуществлялись вручную. Однако современный уровень развития бизнеса предъявляет принципиально новые требования к информационному обслуживанию, в том числе обеспечение скорости передачи информации, ее актуальности, достоверности и своевременности предоставления конечному пользователю. Появление новых технологий организации информационных процессов связано, прежде всего, с использованием компьютерных технологий. Информационные технологии, применяемые в области управления технологическими процессами, могут быть реализованы в виде полностью автоматических информационных систем. В этом случае автоматизированы все процедуры регистрации, сбора, передачи, обработки информации, а также выработка управляющих воздействий, с помощью которых осуществляется управление технической системой. Такие автоматические информационные технологии используются обычно в производственных системах. В частности, к этому классу информационных систем можно отнести так называемые интеллектуальные здания, в которых автоматизированы процессы технической эксплуатации здания, в том числе процессы теплоснабжения, освещения, кондиционирования и т.п.

В системах организационного управления наиболее распространены автоматизированные информационные технологии, в которых выработка управляющего воздействия возложена на человека — лицо, принимающее решение (ЛПР) (8).

Современные информационные системы состоят из нескольких видов обеспечивающих подсистем, к которым относятся: техническое, программное, информационное, организационное, правовое и эргономическое обеспечения.

Техническое обеспечение представляет собой комплекс технических средств, обеспечивающих функционирование информационной системы. В него входят персональные компьютеры, периферийное оборудование (принтеры, сканеры, плоттеры и т.д.), средства коммуникации и связи (модемы, сетевые платы и т.д.), а также средства оргтехники (ксероксы, факсы и т.д.). Средства оргтехники целесообразно включать в техническое обеспечение информационной системы, так как они органично встраиваются в систему сбора, передачи и обработки информации и являются неотъемлемым атрибутом современного офиса. Кроме того, функции принтера, ксерокса, факса выполняет одно устройство. Выбор необходимого состава технических средств должен определяться, прежде всего, функциональными задачами информационной системы и соответствующей предметной областью.

Программное обеспечение — это совокупность программ и документации на них, реализующих основные функции информационной системы. Необходимость разработки собственного программного обеспечения возникает только при решении уникальных задач.

Информационное обеспечение представляет собой совокупность информационной базы предметной области и средств и методов ее обработки. Прежде всего, встают вопросы проектирования информационной базы, которые являются определяющим условием успешной работы всей системы в будущем. Не менее трудоемкой задачей является наполнение информационной базы конкретными данными.

Организационное обеспечение представляет собой комплекс методов и правил организации работы с информационной системой, а также описание должностных инструкций пользователей информационной системы. В сложных информационных системах этот вид обеспечения играет весьма важную роль, так как он определяет порядок функционирования информационной системы. Несоблюдение правил пользования информационной системой, и невыполнение должностных инструкций могут привести к неадекватности базы данных и, как следствие, к принятию неправильных управленческих решений.

Пример. В системах управления гостиничными комплексами несвоевременный ввод информации о состоянии номерного фонда может привести к снижению эффективности работы всей гостиницы.

Правовое обеспечение включает в себя комплекс правовых норм и прав пользователей информационной системы. Эта подсистема обеспечивает ограничение доступа к данным различных категорий пользователей, как правило, путем организации парольного доступа. Кроме того, в настоящее время одними из важнейших вопросов становятся проблемы защиты информации от несанкционированного доступа (3).

Эргономическое обеспечение предполагает разработку рекомендаций и норм правильной организации рабочего места пользователя системы, в том числе правильное расположение компьютеров в помещении, соблюдение необходимого уровня освещенности, установление нормирования работы пользователя за компьютером и т. п.

К современным техническим средствам реализации информационных технологий относятся: персональные компьютеры; локальные и глобальные вычислительные сети; коммуникационные средства; телефонная техника; видеоинформационные системы и др. Современные информационные системы предполагают, как правило, интеграцию различных программных продуктов. В состав информационной системы входят средства для документационного обеспечения управления, информационной поддержки предметных областей, коммуникационное программное обеспечение, средства организации коллективной работы сотрудников и другие вспомогательные технологические продукты. Внедрение информационных технологий предполагает не только автоматизацию основных информационных бизнес-процессов, но иногда и их существенное изменение. Это связано с совершенствованием документооборота в системе, а повышение надежности и оперативности предоставления информации позволяет больше времени уделять ее анализу, а не рутинной обработке.

Внедрение современных информационных технологий должно обеспечивать выполнение ряда требований, в том числе наличие удобного и дружественного интерфейса, обеспечение безопасности с помощью различных методов контроля и разграничения доступа к информационным ресурсам, поддержку распределенной обработки информации, использование архитектуры клиент-сервер, модульный принцип построения систем, поддержку технологий Интернет и т.д.

**2. Применение информационных технологий для обеспечения безопасности клиента**

**2.1 Обеспечение безопасности клиента в гостинице**

Для услуг информационной безопасности на мировом рынке услуг обеспечения защиты составляет около 6%. В России соответствующий показатель не превышает 4%. В то же время отечественный рынок информационной безопасности тесно связан с быстрорастущим рынком системной интеграции, что свидетельствует о его перспективности.

Информационные технологии, обеспечивающих безопасность клиента, используется на объектах разных типов и уровней сложности. Так, на основе этой системы разработан и успешно применяется интегрированный комплекс безопасности для отелей. Он включает в себя системы охранно-пожарной сигнализации, видеонаблюдения, контроля доступа и проезда на парковку. Специализированный программный модуль позволяет автоматизировать взаимодействие системы безопасности и компьютерной системы, управляющей гостиничным комплексом.

Предлагаемое решение обеспечивает безопасность объекта по всем основным направлениям (7):

— видеонаблюдение за всеми помещениями гостиничного комплекса, включая парковку;

— обеспечение пожарной безопасности;

— контроль въезда/выезда автотранспорта, организация работы автопарковок;

— охрана номеров с функцией автоматической постановки и снятия при уходе и приходе гостя;

— контроль доступа гостей в номера, а также к различным дополнительным сервисам отеля (фитнес, конференц-залы и т. д.);

— разграничение доступа персонала в служебные помещения гостиницы, а также учет рабочего времени персонала.

За счет взаимодействия с системой управления гостиницами появляются дополнительные возможности (9):

— при регистрации гостя в гостиничной системе информация о нем автоматически вносится в базу данных, а выдаваемые гостю карты доступа разрешают проход в соответствующие помещения гостиницы;

— при продлении срока проживания гостя срок действия карт также продлевается на соответствующий период;

— при выезде или выселении гостя, выданные ему карты, автоматически аннулируются в системе доступа.

Преимущества и достоинства:

— Повышение общего уровня безопасности гостиничного комплекса (снижается вероятность краж в номерах, актов вандализма и пр.) и, как следствие, повышение лояльности клиентов.

— Возможность оперативного реагирования на конфликтные ситуации, что позволяет избежать серьезных проблем с постояльцами отеля.

Подобные решения реализованы в гостиничном комплексе «Волга», санатории «ВИТЯЗЬ», гостинице «Меридиан», «Атриум Палас Отеле», санатории «Самоцвет», гостинице «Парк Инн», гостинице «Орехово» (Россия) и др.

**2.2 Обеспечение безопасности клиента в аэропорту**

Система безопасности, устанавливаемая в аэропортах, несомненно, должна отвечать самым жестким требованиям. На базе информационных технологий возможно создание подобной многоуровневой системы. В частности, по периметру территории аэропорта устанавливаются датчики охраны и видеокамеры. Для прохода сотрудников на территорию аэропорта устанавливаются турникеты со считывателями, фиксирующими данные с бесконтактной карты. Проезд в аэропорт осуществляется по активным ключам с фиксацией государственных номеров всех въезжающих и выезжающих автомобилей.

Решаемые задачи (2):

— Охранное видеонаблюдение на территории аэропорта, в служебных помещениях, технических ангарах, административных зданиях и на терминалах.

— Охрана периметра территории аэропорта.

— Многоуровневое разграничение доступа сотрудников на территорию аэропорта, в здания, сооружения и служебные помещения; учет рабочего времени сотрудников.

— Контроль проезда автотранспорта с автоматическим определением государственных номеров.

— Видеозапись всех действий и команд диспетчеров и руководителей полетов синхронно со звуком.

— Охранная и пожарная сигнализации во всех помещениях с выводом на центральный пункт охраны.

Преимущества и достоинства:

— Повышение уровня безопасности на территории аэропорта за счет пресечения несанкционированного доступа нарушителей и, соответственно, снижения вероятности совершения террористических актов в аэропортах и с использованием самолетов.

— Повышение качества обслуживания пассажиров за счет усиления трудовой дисциплины персонала.

— Снижение вероятности несчастных случаев и трагедий с участием самолетов, в том числе и за счет минимизации человеческого фактора в обеспечении безопасности полетов.

— Возможность интеграции базы системы охраны с единой базой сотрудников аэропорта.

Подобные решения уже реализованы на следующих объектах: аэропорт «Шереметьево», аэропорт «Кольцово», аэропорт «Туймаада», Международный аэропорт «Казань» (Россия).

Самолеты некоторых авиакомпаний с наибольшей степенью вероятности могут стать объектом для захвата. Американские авиакомпании, западногерманская Люфтганза, израильская Эль Ал известны тем, что на борту самолетов, принадлежащих этим авиакомпаниям, обеспечивается очень высокий уровень безопасности.

Такой уровень достигнут в связи с тем, что в прошлом они неоднократно выбирались террористами в качестве объектов для нападения. Самолеты национальной авиакомпании Индии стали объектом захвата сикхских террористов, а кувейтская национальная авиакомпания - шиитами. Наиболее безопасными с этой точки зрения считаются самолеты авиакомпаний таких стран, как Швеция, Швейцария, Сингапур, Гонконг, которые не являются членами крупных политических блоков и не вовлечены в конфликты локального характера. Несмотря на то, что уровень сервиса на самолетах авиакомпаний некоторых коммунистических стран несколько ниже, эти самолеты гораздо реже выбираются объектами для нападения, чем самолеты, принадлежащие авиакомпаниям стран свободного мира. Также примите к сведению, что авиакомпании стран третьего мира, а также небольшое число авиакомпаний промышленно развитых государств имеют очень плохую репутацию с точки зрения обеспечения безопасности.

Комплекс применяемых мер по обеспечению авиационной безопасности в аэропорту и используемые передовые информационные технологии позволяют обеспечивать спокойную и безопасную обстановку на территории аэровокзального комплекса, а также полную сохранность грузов и багажа (1).

**Заключение**

Понятие «безопасность» становится все более актуальным в нашей деловой и повседневной жизни. Мы начинаем понимать под обеспечением безопасности не только защиту от угроз физических, но и предотвращение и учет всевозможных рисков. Экономические, социальные, юридические риски требуют учета и контроля. Таким образом, системы обеспечения безопасности постепенно превращаются в комплексы, позволяющие контролировать многие параметры объектов и процессы, на них происходящие.

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, разработчики предлагают новые концепции и методики.



Естественно, при таком большом потоке информации, который формирует система комплексной безопасности, возникает необходимость в интеграции элементов и систем в единый комплекс, позволяющий контролировать его и управлять им с одного рабочего места. В противном случае информативность поступающей информации сильно снижается, возникают проблемы с оперативностью реагирования службы безопасности на возникающие угрозы, нет возможности оперативно сопоставить информацию из архивов событий разных подсистем.

Из сказанного выше можно сделать вывод, что при существующих потребностях в функциональных возможностях систем обеспечения безопасности, интегрированные комплексы в ближайшее время будут доминировать на рынке безопасности.

**Список литературы**

1. Биржаков М.Б. Введение в туризм. СПб. 2003
2. Вопросы расследования преступлений. Справочное пособие. 2-е издание, М.,1997. С.41
3. Семин В.С. Организация международного туризма. М.: "Финансы и статистика", 2000
4. Безопасность посредством партнерства, NATO Public Diplomacy Division, Brussels, 2005.
5. Поменский Э. Формула безопасности. М., 1991
6. Молчановский В.Ф. Безопасность - атрибут социальной системы // Анализ систем на пороге 21-го века: теория и практика // Материалы международной конференции. М, 1997.Т. 4. Кн. 1.
7. Громов Г.Р. Очерки информационной технологии. М.: Инфо Арт, 1992.
8. Корюшкова А.А. Информационный рынок: продукция, цены и ценообразование. М.: Коринф, 1992.
9. Свириденко С.С. Современные информационные технологии. М.: Радио и связь, 1989.
10. Технология электронных коммуникаций. Т.5: Стандартизация электронных документов и методов их обработки. М: Экотрендз, 1991.
11. Управление. Информация. Интеллект /Под.ред А.И. Берга, Б.А. Бирюкова, Е.С. Геллера, Г.Н. Поварова. М.: Мысль, 1976.
12. Урсул А.Д. Информатизация общества. Введение в социальную информатику. М.: Гл. ред. при АОН, 1990.