Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«**СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ**»

Институт торговли и сферы услуг
Кафедра гостиничного дела

УТВЕРЖДАЮ
Заведующий кафедрой
_____ М. Д. Батраев
подпись инициалы, фамилия
« _____» _____ 2022 г.

БАКАЛАВРСКАЯ РАБОТА

43.03.03 Гостиничное дело
код и наименование направления подготовки

43.03.03.02.01 Ресторанное дело
код и наименование профиля подготовки

Особенности использования информационных технологий в обеспечении безопасности гостиницы на примере гостиницы «Берега»
тема

Руководитель _____ доцент, канд.техн.наук Т. Н. Сафронова
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ Р. Р. Ризванов
подпись, дата инициалы, фамилия

Нормоконтролер _____ Т. Н. Сафронова
подпись, дата инициалы, фамилия

Красноярск 2022

Содержание

Введение

Развитие туризма в мире предъявляет особые требования к объектам размещения. Помимо видимого уровня сервиса устанавливаются нормы безопасности гостиниц и развитие технологий способствует соблюдению этих норм.

Гостиница является местом повышенного скопления людей это накладывает обязательства по обеспечению безопасности гостей на персонал.

Безопасность – состояние объекта защиты, при котором воздействие на него всех потоков вещества, энергии и информации не превышает максимально допустимых значений. Безопасность гостей, персонала, а также защита информации, одна из важнейших проблем, которую должно решить руководство отеля.

Система безопасности предприятия призвана выполнять определенные функции. К наиболее значимым из них следует отнести: прогнозирование, выявление, предупреждение, ослабление опасностей и угроз; обеспечение защищенности деятельности предприятия и его персонала, сохранности его имущества, создание благоприятного конкурентной среды, ликвидация последствий нанесенного ущерба и т.д.

Современный этап развития общества характеризуется интенсивной информатизацией всех сфер его жизнедеятельности. Развитие и широкое

применение информационных технологий является глобальной тенденцией мирового развития и научно-технической революции последних десятилетий.

Информационные технологии используются повсеместно в нашем мире и гостиницы не являются исключением. Они используются как для обеспечения скорости и удобства процесса обслуживания, так и для защиты гостей.

В гостинице можно выделить множество источников опасности, такие как техногенные катастрофы, кражи, пожары, отравления, землетрясения, теракты, хакерские атаки и многое другое. Техническое обеспечение помогает персоналу гостиницы поддерживать безопасность гостей 24 часа в сутки.

В данной работе рассматриваются особенности использования информационных технологий в обеспечении безопасности гостиничных предприятий.

Проблема данного исследования определяется противоречием между потребностями в безопасности, которые предъявляют потенциальные потребители туристских услуг, к индустрии гостеприимства и готовностью средств размещения удовлетворить эти потребности.

Цель исследования: рассмотреть особенности использования информационных технологий в обеспечении безопасности проживающих в гостинице «Берега» г. Красноярска.

Для достижения цели необходимо решить следующие задачи:

1. Рассмотреть основные положения по обеспечению безопасности в гостинице.

2. Рассмотреть роль системы контроля и управления доступом в обеспечении безопасности гостиниц.

3. Рассмотреть систему защиты информации.

4. Рассмотреть комплекс технических средств по противопожарной защите.

5. Рассмотреть комплекс технических средств, обеспечивающих охранную сигнализацию и видеонаблюдение.

6. Предоставить информацию для общего представления о гостинице «Берега».

7. Исследовать использование информационных технологий в системе безопасности гостиницы «Берега».

8. Предложить комплекс мер для улучшения деятельности гостиницы «Берега».

Объектом исследования является гостиница «Берега» г. Красноярск

Предмет исследования: информационные технологии в системах безопасности гостиницы «Берега» г. Красноярск

Методы исследования: наблюдение, изучение литературных источников, анонимное интервью с персоналом гостиницы.

Общий объем работы составляет 62 страницы. Работа состоит из трех разделов и иллюстрирована 3 таблицами и 27 рисунками.

1 Теоретические основы использования информационных технологий в системах безопасности гостиниц

1.1 Основные положения по обеспечению безопасности в гостинице.

Безопасность — состояние защищённости жизненно важных интересов личности, общества, государства от внутренних и внешних угроз, либо способность предмета, явления или процесса сохраняться при разрушающих воздействиях. За безопасность в гостиницах отвечает служба безопасности. Главной их целью является предотвращение воздействия любого вида опасностей на гостей.

В гостинице можно выделить следующие источники угроз:

1. Действия асоциальных и преступных элементов. Сюда относятся кражи, мошенничество, хулиганство, нарушения общественного порядка, теракты и прочее.

2. Пожароопасные ситуации. Сюда относится угроза пожара в следствии неправильного обращения гостей или персонала с воспламеняющимися предметами, а также неисправности газового оборудования, используемого на кухне и электропроводки.

3 Техногенные факторы. Сюда входят аварии бытового электрического оборудования, неисправности систем водоснабжения, прорывы отопительных систем.

4. Природные катастрофы. Сюда относят цунами, землетрясения и другие [17].

Информационные технологии – это процесс, использующий совокупность средств и методов сбора, обработки и передачи данных для получения информации нового качества о состоянии объекта, процесса или явления.

Информационные технологии помогают снизить риски и ущерб опасных ситуаций. У технические средства имеют ряд особенностей, делающих их использование крайне выгодным:

- Неподверженность усталости, болезням, невнимательности и погодным условиям.
- Неподкупность, невозможность обмана, шантажа или запугивания.
- Точность выполнения заложенных функций, мгновенная реакция.

Технические средства информатизации (ТСИ) — это совокупность систем, машин, приборов, механизмов, устройств и прочих видов оборудования, предназначенных для автоматизации различных технологических процессов информатики, причем таких, выходным продуктом которых является информация (данные), используемая для удовлетворения информационных потребностей в разных областях деятельности общества [26].

Технические средства являются частью обширного комплекса информационных технологий. Они находятся в ведении IT – департамента и службы безопасности. IT – департамент следит за работоспособностью технических средств, а служба безопасности использует данные системы.

Эффективность технических средств делает рациональным выбор комплексного подхода в обеспечении безопасности гостиницы. Этот подход учитывает наилучшее сочетание технических и физических мер реагирования и предотвращения на опасные ситуации.

В гостинице можно выделить несколько групп технических средств безопасности:

1. Система пожарной безопасности. К этой группе можно отнести все технические средства обнаружения, предотвращения и информирования о пожарах на территории гостиницы. Структура представлена следующими компонентами: система пожарной сигнализации, система визуально звукового оповещения, система пожаротушения, система управления вентиляцией и дымоудаления.

2. Система контроля и управления доступом. Данная система отвечает за санкционированный и беспрепятственный доступ к различным помещениям гостиницы и предотвращение неправомерного доступа.

3. Система защиты информации. Данная система отвечает за защиту от неправомерного получения информации из гостиничных асу и баз данных о гостях, платежных данных, документов внутреннего пользования и другой информации, не подлежащей разглашению.

4. Системы наблюдения. Сюда относятся технические средства, отвечающие за обеспечением видеонаблюдения на территории гостиницы.

5. Системы охранной сигнализации. Данная система отвечает за обнаружение фактов несанкционированного проникновения в помещения гостиницы.

Каждая из систем безопасности гостиницы связана с другими и не может функционировать отдельно, для достижения цели работы необходимо рассмотреть особенности использования каждой из систем, описать её структуру, особенности использования и значения, данные задачи раскрыты в следующих подпунктах работы, однако не следует воспринимать каждый из них обособленно, так как например, система контроля и управления доступом не может функционировать без системы оповещения о несанкционированных проходах относящейся к системе охранной сигнализации [20].

1.2 Роль системы контроля и управления доступом в обеспечении безопасности гостиничного предприятия

СКУД – механизм отслеживания входа и выхода в помещения, состоящий из преграждающего устройства, идентификатора, считывателя и контроллера. В свою очередь контроллер часто может быть соединен с АСУ гостиницы. СКУД регулирует правомерность прохода во все помещения гостиницы. Сюда входят не только номера гостиницы, но и технические помещения.

СКУД имеет ряд очевидных преимуществ перед использованием физических систем запирания:

- Идентификация лица, проходящего на территорию.
- Простота создания ключей, скорость их выпуска.
- Учет рабочего времени для персонала.
- Расчет заработной платы для персонала.
- Интеграция с АСУ.
- Интеграция с «умными устройствами».
- Интеграция с системами безопасности.

Существует три режима работы СКУД:

Автономный – контроллер и замок не связаны с сервером, работают как отдельные устройства, и не позволяют менять ключи удаленно, такой вариант самый дешевый, однако не позволяет собирать много информации о том, кто посещал помещения, время посещения и прочее.

Комплексный – открытием дверей занимается сервер, мгновенно получающий информацию о том, кто, куда и когда зашел, такой вариант самый распространенный.

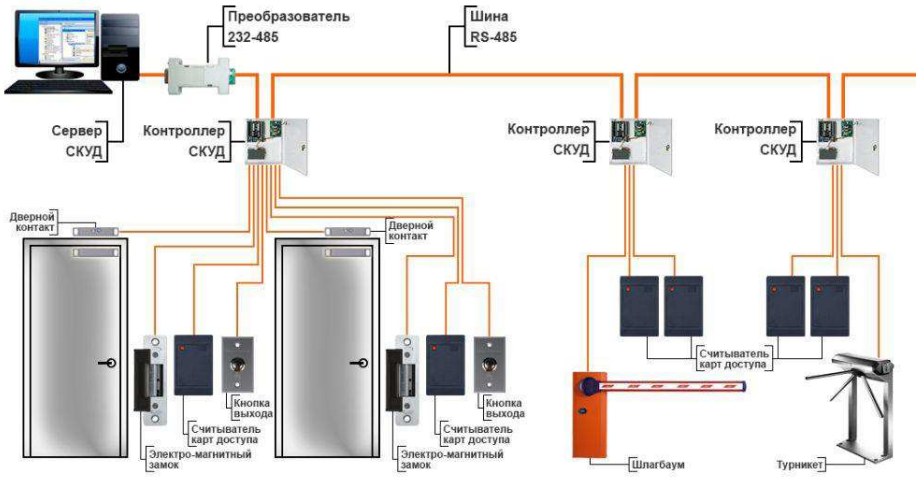


Рисунок 1 – Состав системы контроля и управления доступом

Комбинированный – открытием дверей занимается контроллер как при автономном режиме, данные о работе отправляются на сервер в реальном времени, как при комплексном [6].

Видимой частью СКУД являются преграждающие устройства. В гостиницах на двери номеров устанавливаются электромеханические замки. Для технических и подсобных помещений устанавливаются электрозащёлки. Электромагнитные замки чаще всего устанавливаются на двери пожарных выходов, так как данный вид замков запирается напряжением. Помимо дверей к СКУД относятся ворота и шлагбаумы, которые могут быть как автоматическими, со считывателями номеров, так и открываемые человеком – оператором [7].

Рисунок 2 – Электромагнитный и электромеханический замок

Для преодоления преграждающих устройств используются идентификаторы. Наиболее используемыми идентификаторами являются – карточка, брелок и метка. Также идентификатором может быть кодовый замок, однако это не так безопасно, поскольку невозможно определить конкретное лицо, проникающее в помещение, также код может быть узнан третьими лицами.

Карты брелок и метки имеют несколько вариантов связи со считывателем. Первый – карты с магнитной полосой, данный вид идентификации является устаревшим и неудобным. Карты содержат меньше информации, их тяжелее перезаписывать, они имеют свойство

размагничиваться, а также дороже в исполнении. Второй вариант с RFID – метками является более предпочтительным, так как такие метки дешевле в исполнении, могут быть исполнены не только в форм-факторе карт, но и меток, брелков, которые могут оставаться у гостей в качестве сувениров, также такие метки может держать в себе больше информации и не размагничиваются. Помимо этих двух вариантов существуют proximity карты, такие карты используются в меньшей степени, так как отсутствует возможность перезаписи, а также такие карты легче подделать.

Рисунок 3 – Идентификаторы proximity-card, магнитная карта, карта с RFID-меткой

Помимо вышеуказанных существуют биометрические идентификаторы, однако для гостиниц они не так востребованы, поэтому рассматривать их в рамках работы не целесообразно.

Идентификаторы распознаются считывателем. Считыватель – устройство, передающее информацию с идентификатора на контроллер. В случае с магнитными картами, считыватель представлен карт-ридером, для proximity карт – электронная плата с антеной, для RFID меток – два электрических контакта в виде «лузы»

Контроллер – самая важная часть системы, в него заложена база кодов идентификаторов, с которой сверяются метки, если метка есть в базе контроллера, то человек получает доступ к помещению. Контроллеры соединены в сетевую базу, интегрированную с АСУ гостиницы, поэтому зарегистрированный на ресепшене ключ гостя, мгновенно заносится в базу

контроллера его номера и обеспечивает доступ гостя к номеру. Контроллеры в большинстве случаев имеют собственный аккумулятор, либо запитаны от источников дополнительного питания, чтобы обеспечивать доступ к номеру в случаях перебоя сетей электроснабжения.

Также следует отметить следующие преимущества электронной СКУД – самое важное, все данные о перемещениях в гостинице записываются, это предотвращает большинство краж в номерах и «левые поселения». СКУД также исключает человеческий фактор в процессе аудита замков. Кроме прочего данная система отлично интегрируется с системой пожарной безопасности, так при пожаре все аварийные выходы могут быть открыты в автоматическом режиме и предотвратить панические действия среди людей, находящихся в гостинице [8].

1.3 Роль технических средств противопожарной защиты

Пожарная безопасность — набор практических мер и правил, направленных на предотвращение возникновения случайного или преднамеренного пожара, ограничение его распространения в случае возникновения и минимизацию последствий, включая возможные потери, до приемлемого уровня.

Гостиница является местом большого скопления людей поэтому к ней применяются повышенные меры противопожарной безопасности, существует ряд нормативных актов, регламентирующих требования к гостиницам, туда входят как нормы проектирования, использования различных материалов, так и использование технических средств пожарной безопасности.

Технические средства пожарной безопасности имеют 4 функции:

- Обнаружение пожара
- Оповещение о пожаре
- Предотвращение пожара

- Тушение пожара

Обнаружение пожара возлагается на пожарные датчики. Пожарные датчики бывают автоматические и ручные. Ручные представляют из себя кнопку, которую следует нажимать при обнаружении пожара, если автоматические датчики ещё не среагировали

Рисунок 4 – Ручной пожарный датчик

Автоматические датчики считают информацию об изменяющихся параметров в помещении, на основании чего происходит срабатывание. Автоматические датчики бывают дымовые, тепловые и инфракрасные.

Дымовые датчики работают по принципу выявления в воздухе твердых частиц, образующихся в процессе горения. Тепловые датчики работают на изменение температуры в помещении, если температура превышает допустимую норму, то датчик срабатывает. Инфракрасные датчики регистрируют спектр открытого пламени, реакция такие датчики срабатывают быстрее всего, однако источники жесткого излучения, такие как фотовспышки или электрогазосварочное оборудование могут вызывать у данных датчиков ложные срабатывания [3].

Рисунок 5 – Датчики пожарной сигнализации дымовой, тепловой, инфракрасный

Каждый из датчиков имеет ряд преимуществ и недостатков, поэтому в одном помещении могут использоваться сразу 2 вида датчиков, либо используются комбинированные.

Датчики отправляют сигнал на приемное оборудование, задачей приемного оборудования является разделение сигнала по зонам возгорания. По этому параметру приемное оборудование бывает малозонное и многозонное. Малозонное контролирует от 2 до 16 зон и применяется в малых и средних отелях. Многозонные же используются в крупных отелях. Современные приемно-контрольные устройства относительно недороги и модернизируемы путем подключения дополнительных модулей, что позволяет оборудованию в автоматическом режиме управлять пожарной сигнализацией, системой вентиляции и системами пожаротушения.

Приемное оборудование принимает решение о включении пожарной сигнализации, а также защищает от ложных срабатываний. Приемное оборудование имеет несколько типов работы: пороговая, адресно-опросная, адресно-аналоговая.

Пороговый – самый дешевый вариант. Суть его в том, что датчик при превышении допустимого порога одного из параметров отправляет на приемное оборудование сигнал. Однако Приемное оборудование не может из-за особенностей подключения определить точный источник возгорания.

Адресно-опросное оборудование такой тип работы заключается в постоянном опросе датчиков, а не просто ожидание сигнала от них. Оно

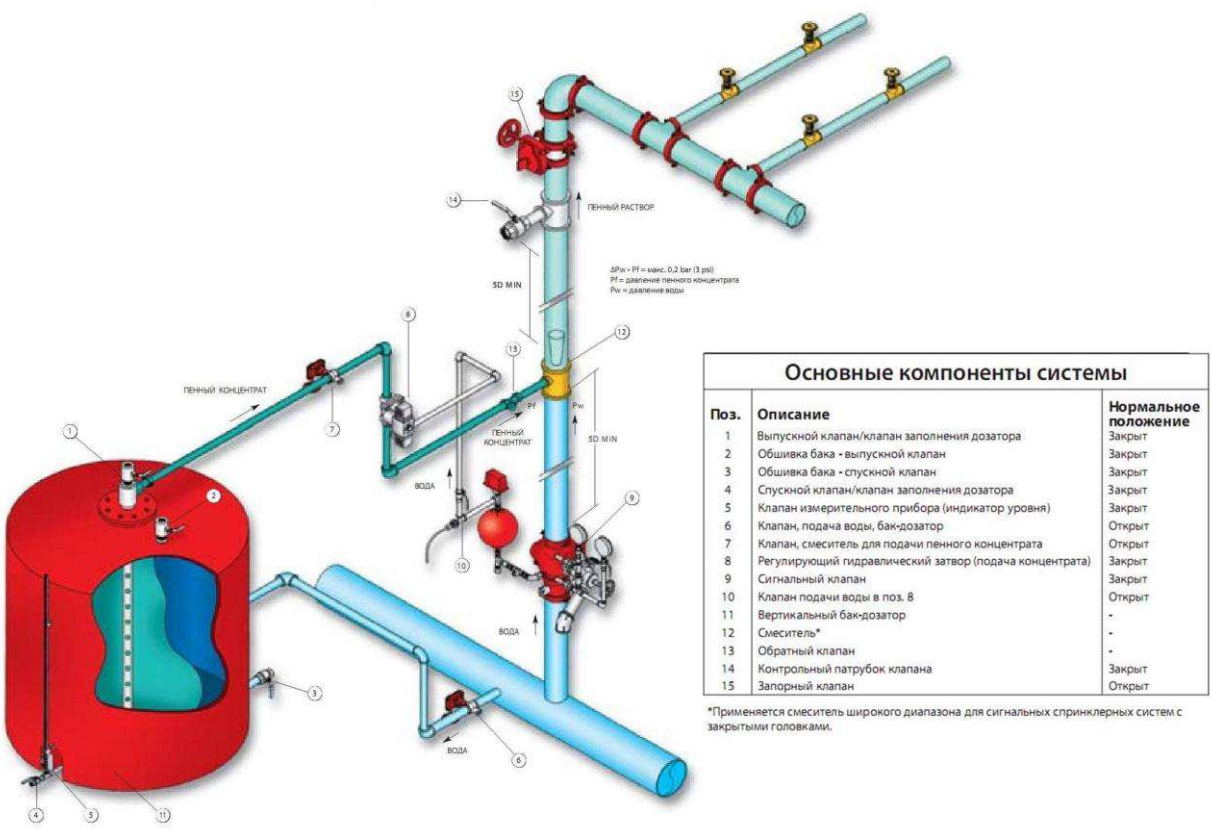
определяет одно из трех состояний датчика (норма, пожар, неисправность). В такой системе каждому датчику присвоен свой адрес, это позволяет точно узнать место пожара и состояние каждого конкретного датчика.

Адресно-аналоговое оборудование. Такой тип сигнализации наиболее совершенен, он имеет такой же функционал, как и адресно-опросное оборудование, однако в пороговой и адресно-опросной сигнализации датчик подает информацию на контрольную панель о включении сигнализации, в аналоговой сигнализации подаются измеряемые параметры, на основе которых контрольная панель принимает решение о состоянии пожара. Такой тип сигнализации наиболее совершенен и потому он самый дорогой и не смотря на его дороговизну отели используют его чаще всего [15].

Пожарная сигнализация служит для оповещения для гостей и персонала о случаях пожара в гостинице. Согласно ТехРегламенту о требованиях пожарной безопасности пожарной сигнализацией оборудуются все гостиницы без исключения. Из-за вероятности ложного срабатывания, сигнал о пожаре сначала подается в диспетчерскую службы безопасности, где дежурный принимает решение об оповещении гостей. Для оповещения гостей используются световые, звуковые и речевые пожарные оповещатели. Они должны располагаться на видных местах, чтобы каждый гость незамедлительно был информирован о пожаре [28][29].

Когда пожар обнаружен включаются системы пожаротушения. Всего существует 4 вида систем пожаротушения: водяная, газовая, пенная и порошковая. Однако газовая, пенная и порошковая системы могут представлять опасность для неподготовленного человека, в связи с этим в гостиницах используются только водяные системы, они же спринклерная. Спринклерная система представляет из себя ороситель, устанавливаемый на сети водопроводных труб, которые всегда находятся под давлением воды. Ороситель мелкими каплями разбрызгивает воду на область пожара, вследствие чего образуется водяной туман, тушащий, либо замедляющий пожар.

Во время пожаров большое количество людей страдает не от ожогов, а от отравления продуктами горения, для предотвращения таких случаев в гостиницах используются системы дымоудаления. Система дымоудаления является частью системы пожарной безопасности в здании и представляет собой комплекс средств по ликвидации дыма и по обеспечению притока чистого воздуха внутри помещения. Дымоудаление предполагает очищение воздуха не только от дыма, но и от пепла и опасных для жизни и здоровья газообразных веществ. Система дымоудаления монтируется в длинных коридорах, холлах, гардеробных, иных местах общего пользования с большой площадью.



Основные компоненты системы

Поз.	Описание	Нормальное положение
1	Выпускной клапан/клапан заполнения дозатора	Закрыт
2	Обшивка бака - выпускной клапан	Закрыт
3	Обшивка бака - спускной клапан	Закрыт
4	Спускной клапан/клапан заполнения дозатора	Закрыт
5	Клапан измерительного прибора (индикатор уровня)	Закрыт
6	Клапан, подача воды, бак-дозатор	Открыт
7	Клапан, смеситель для подачи пенного концентрата	Открыт
8	Регулирующий гидравлический затвор (подача концентрата)	Закрыт
9	Сигнальный клапан	Закрыт
10	Клапан подачи воды в поз. 8	Открыт
11	Вертикальный бак-дозатор	-
12	Смеситель*	-
13	Обратный клапан	-
14	Контрольный патрубок клапана	Закрыт
15	Запорный клапан	Открыт

*Применяется смеситель широкого диапазона для сигнальных спринклерных систем с закрытыми головками.

Рисунок 6 - Спринклерная система пожаротушения

СДУ представляет собой комплекс вентиляционных шахт, в которых путем создания перепадов давления воздуха дым выводится из здания гостиницы [1].

Также в блоке технических средств пожарной безопасности стоит освятить защиту от одной из самых частых причин пожаров – короткое замыкание. В рамках работы умолчим о стандартном регламенте обслуживания и проверке проводки на предмет работоспособности и перейдем сразу к защитным техническим средствам позволяющим предотвратить пожары на этой почве.

В первую очередь это самый обычный автоматический выключатель используемый повсеместно. Его принцип работы крайне прост, при прохождении слишком большого количества тока металлическая пластина внутри выключателя нагревается и автоматический выключатель срабатывает.

Помимо таких простейших выключателей существуют более продвинутые работающие по более сложному принципу.

Автомат с электромагнитным расщепителем имеет соленоид внутри, из которого под воздействием большой силы тока выталкивается сердечник.

Устройства дифференциальной защиты, являются еще более усовершенствованными, так как в них используется 2 проводника на которых сравнивается сила тока, и при утечке, которая происходит в случае утечки или короткого замыкания, подача тока прекращается.

Ограничитель мощности.

Следующий прибор отключает нагрузку в случае превышения мощности. Это Реле ограничения мощности. Хоть это устройство и не является по своей сути защитным и его используют в большей степени энергосбытовые или сетевые компании для контроля и ограничения потребления электроэнергии, свыше установленной в нормальной или уменьшения этой величины в аварийной ситуации. Изделие отслеживает потребляемую мощность и в случае её превышения отключает потребителя.

Данные устройства защищают приборы и проводку от короткого замыкания и утечки тока [11].

Также в этом разделе следует сказать об интеграции ОПС – охранной пожарной сигнализации со СКУД, сейчас разберем только пожарную систему, в следующем пункт данный вопрос будет рассмотрен с другой стороны.

Во-первых, аппаратная база данных систем сильно схожа, это значит, что могут использоваться универсальные блоки управления и контрольные панели, что существенно экономит время и деньги. Функционал контроллеров СКУД больше, чем у ОПС, это значит, что он может предоставлять более подробную информацию о произошедших событиях. Например, ложное срабатывание спринклерной системы может повредить имущество, и в дешевой ОПС, не будет подробной информации об этом событии, однако в более продвинутых интегрированных блоках управления останется информация, ручной пуск ли это, или ложное срабатывание.

Во-вторых, важным преимуществом интеграции этих двух систем является автоматическая разблокировка всех дверей в случае пожара. Что способствует более эффективной эвакуации людей в экстренных обстоятельствах.

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. Разблокировка дверей на случай чрезвычайной ситуации настраивается через программную интеграцию — как реакция на событие [3][10].

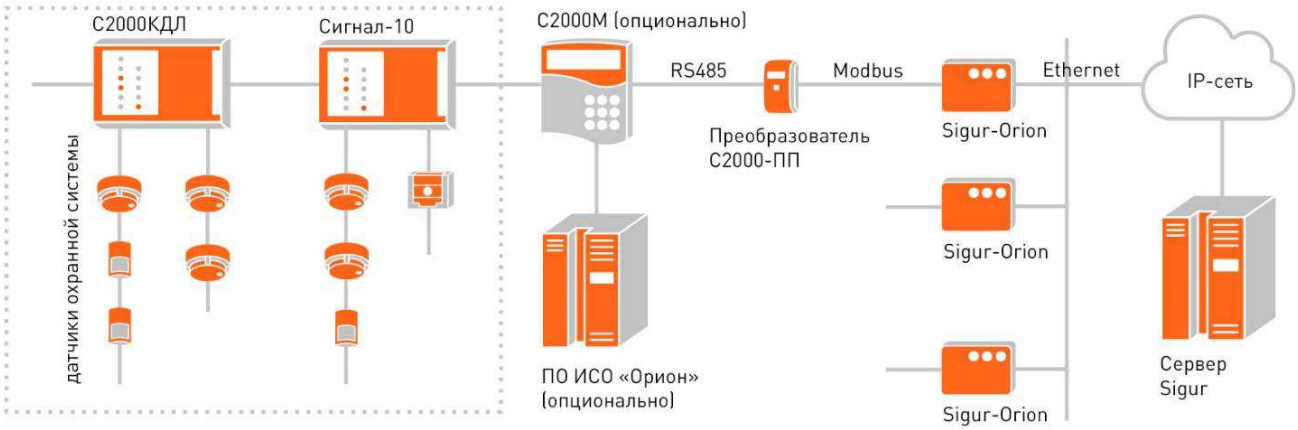


Рисунок 7 – Архитектурная схема интеграции на примере СКУД и ОПС «Болид»

1.4 Роль охранной сигнализации и технических средств видеонаблюдения

Охранная сигнализация и видеонаблюдение являются частью системы контроля доступа на объект, если СКУД направлен на предотвращение случаев несанкционированного доступа, то охранная сигнализация (ОС) – направлена на обнаружение таких случаев и оповещение о них службы безопасности гостиницы [13].

В гостинице защитой охранной сигнализацией подлежат следующие помещения касса, камера временного хранения багажа, сейф для ценностей, кабинеты администрации гостиницы, аппаратные и пультовые прочие ответственные служебные помещения, а также гостиничные номера.

Система охранной сигнализации может быть автономная, либо с подключением к пульту централизованного наблюдения (ПЦН). В первом случае датчики соединены сразу с сиреной и сигнал никуда не уходит, такая система дешевле, однако менее эффективна.

Состав системы охранной сигнализации:

- Контрольная панель.
- Устройство управления.
- Сигнальные устройства.

- Датчики.

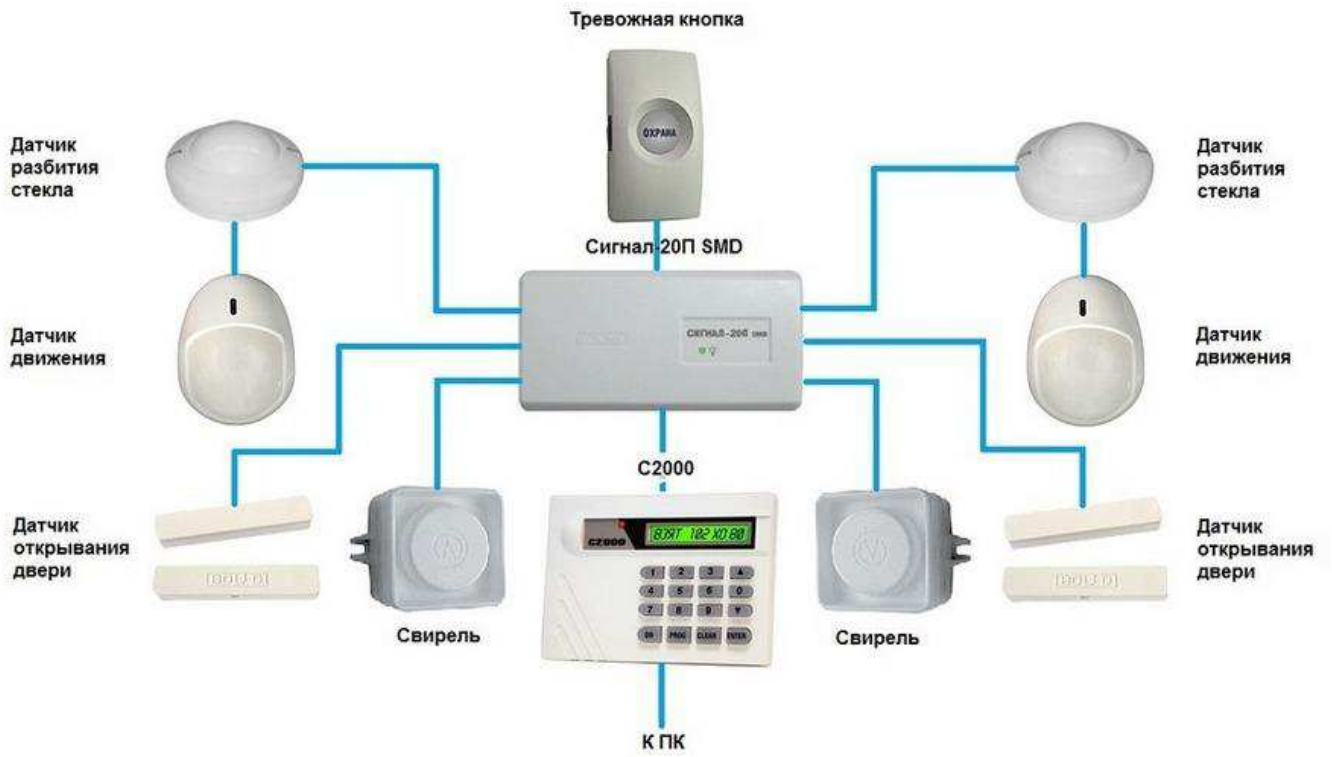
Контрольная панель является мозгом охранной сигнализации, она постоянно опрашивает состояние датчиков (норма/тревога). По заданным алгоритмам работы охраняемые зоны не равнозначны. Так при срабатывании датчиков в определенных зонах сигнализация не включается сразу. Таких зоны 4: проходная, мгновенная, тамперная, 24-х часовая.

Проходная зона включает путь от входа до управления сигнализацией, задержка тревоги происходит при последовательном срабатывании определенного порядка датчиков.

Мгновенная зона, это зона при получении сигнала из которой незамедлительно активируется сигнализация.

Тамперная зона выражена не помещениями, а конкретными объектами, такими как сейфы, важное контрольное оборудование, витрины и др.

24-х часовая зона, отличается мгновенным срабатыванием сигнализации, в отличии от мгновенной эта зона не может быть в не охраняемом режиме,



сюда как правило, включаются тревожные кнопки вызова служб экстренного реагирования [22].

Рисунок 8 – Состав охранной сигнализации

Важно отметить, что контрольная панель может быть интегрирована с контроллерами СКУД.

Взаимодействие ОПС и СКУД. В первую очередь, это возможность переложить ответственность за постановку помещений на охрану на тех людей, кто пользуется этими помещениями. Вовсе не обязательно, чтобы на каждом помещении стоял считыватель, и при входе в комнату она снималась с охраны. Это действительно довольно дорого. Достаточно настроить один турникет на входе так, чтобы при проходе Иванова снималась с охраны комната 203, а при проходе Сидорова или Петрова – комната 115. Чем это лучше? Иначе, как обычно бывает, пришел Иванов – ранняя пташка – в 5 часов утра на работу, дежурный снял с охраны все здание. И все комнаты на всех этажах стоят без охраны. Да, по идее, ваши охранники обязаны под роспись каждому выдать ключ и после этого снять с охраны одну его комнату. На самом деле, они банально не успевают отслеживать всех проходящих, так, присматривают, чтобы ключи брали знакомые лица, а уж кто какой ключ взял – это слишком сложно. Тем более сложно снимать с охраны комнаты по одной, перепутаешь – шуму будет много, куда проще снять все сразу, все равно никто разбираться не будет. Автоматика на то и автоматика, что она не устает и никогда ничего не перепутает. А освобожденный от рутины охранник наконец действительно сможет внимательнее присмотреться к тому, кто куда проходит [19][10].

Для взаимодействия с контрольной панелью используются: клавиатура, располагаемая на контрольной панели или непосредственно рядом с ней; носимый радио-брелок; электронные ключи аналогичные СКУД.

Контрольная панель принимает решения на основе информации с сигнализационных датчиков.

Ассортимент сигнализационных датчиков, использующихся для обнаружения фактор проникновения, крайне разнообразен, можно сгруппировать их по типу защищаемого объекта:

- Датчики, используемые на дверях (магнитоконтактные, вибрационные, инфракрасные)
- Датчики используемые на стеклах (акустические, вибрационные)
- Датчики, использующиеся во внутренних помещениях (инфракрасные, микроволновые, ультразвуковые, комбинированные)
- Датчики, использующиеся на отдельных предметах, таких как сейфы, витрины, шкафы с оружием (емкостные, вибрационные)

При переходе в режим тревоги включаются сигнальные устройства. Сигнальные устройства делятся на следующие типы:

- Звуковые.
- Строб-вспышки.
- Комбинированный.
- Голосовые дозваниватели.
- GSM модем.
- Цифровые коммуникаторы [3].

Вторым аспектом контроля доступа и обнаружения несанкционированного доступа является система видеонаблюдения.

Система видеонаблюдения выполняет ряд функций в гостиничном предприятии:

- Обнаружение краж.
- Контроль обстановки всех территорий и помещений в аспекте безопасности людей.
- Выявление угроз техногенного характера.
- Контроль гостей постояльцев.
- Определение обоснованности недовольств постояльцев.
- Контроль входа/выхода.
- Уменьшение количества работников СБ.

В состав системы видеонаблюдения в гостинице входят устройства записи изображения, элементы фиксации кадра, источники освещения, кабельная продукция, источники основного и резервного питания, средство передачи данных, мониторы и другое дополнительное оборудование.

Возможности системы видеонаблюдения в гостинице

- Постоянный мониторинг и непрерывная видеозапись в реальном времени.
- Запись видеоархива по детектору движения.
- Интеграция системы видеонаблюдения с ОПС и тревожными датчиками с оперативной проверкой, является тревога реальной или ложной.
- Получение всей статистики по проходам: как гостей отеля, так и персонала гостиницы.
- Идентификация личности гостей и персонала.

Устройства записи изображения – видеокамеры, они бывают двух видов аналоговые и ip-камеры. Отличий между камерами весьма много. IP-камера это отдельная система со своим адресом, это дает ей как преимущества, так и недостатки в первую очередь, она дешевле, чем аналоговая камера, может использовать беспроводное подключение и не требует дополнительных модулей. Аналоговые камеры, требуют дополнительного оборудования в виде поворотных модулей, модулей дополнительного освещения, квадарторов, сменных линз и специального софта. Помимо этого, аналоговые камеры могут настраиваться более тонко, включаться от датчиков движения, настраивать светочувствительность и другие настройки.

Камеры отправляют изображение на видеорегистратор, он преобразует и сохраняет видеосигнал с видеокамер, к одному регистратору подключается от 2 до 64 камер.

Квадартор выводит изображение на мониторы, с регистратора, а также дает картинку с нескольких камер в реальном времени. Некоторые регистраторы имеют в себе функции квадарторов.

Монитор используется дежурным для получения изображения с камер и конфигурирования устройств видеонаблюдения.

Основные зоны видеонаблюдения в отеле:

- Периметр территории.
- КПП, проходная, пост охраны, диспетчерская.
- Главный и служебный входы.
- Коридоры с номерами.
- Лифтовые холлы.
- Технические помещения.
- Зоны общего пользования (рестораны, бары, лобби, конференц-залы).
- Зоны расположения кассовых терминалов.
- Склады, кладовые гаража.
- Автостоянки, парковки .
- И другие помещения по рекомендации службы безопасности [22].

В настоящее время охранно-пожарная сигнализация, СКУД и система видеонаблюдения, благодаря универсальному оборудованию интегрируются в единую систему безопасности отеля образуя целостную экосистему. Основным преимуществом подобной интеграции является то, что ведется единая база данных всех систем (к событию СКУД или ОПС "привязана" определенная видеозапись) и оборудуется единое рабочее место, куда стекается вся информация и отображается в удобном виде. Это позволяет одному-двум сотрудникам службы безопасности контролировать крупный объект и значительно снижает эксплуатационные расходы (персонал и техническая эксплуатация) [8].

Интегрированные системы позволяют реализовать различные сценарии событий, к примеру, при обнаружении системой виденаблюдения (с функциями видеоаналитики) проникновения на объект постороннего человека и при отсутствии в течении установленного времени реакции оператора на тревожное

событие – начальнику охраны будет передано тревожное сообщение на мобильный телефон и, к примеру включиться наружное освещение обьекта и т.п. [10].

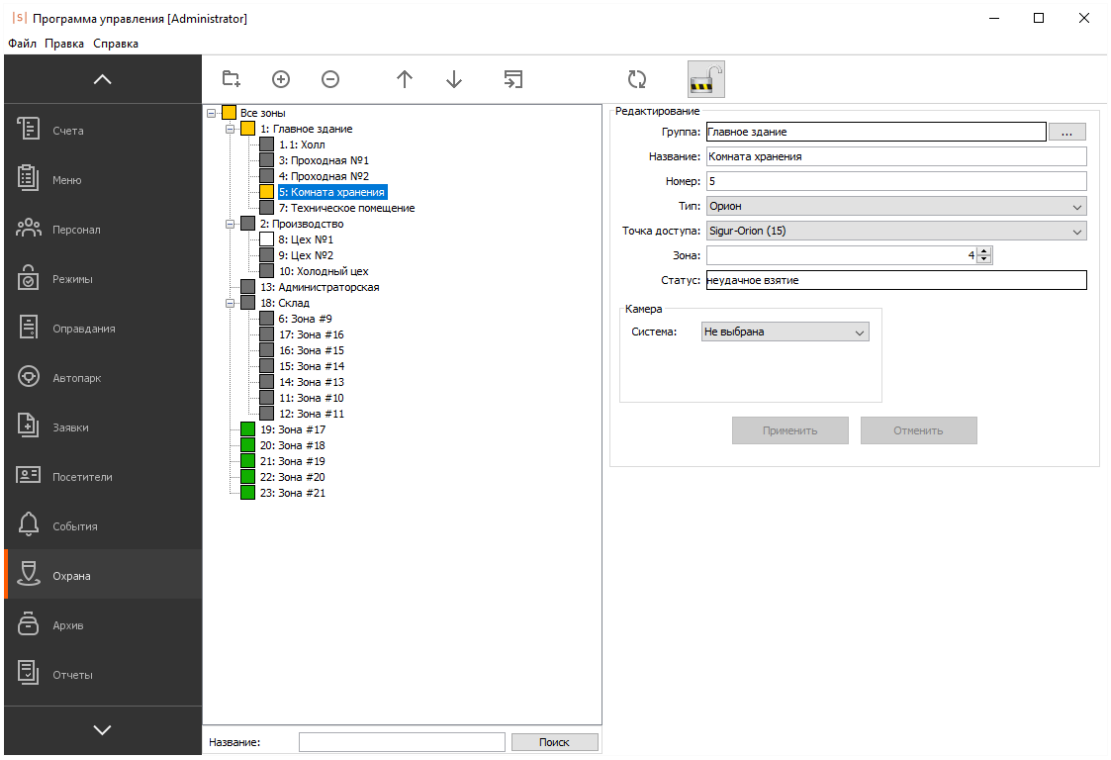


Рисунок 9 – Интерфейс интегрированной охранной системы Sigur

1.5 Роль системы защиты информации

Большой объем данных о посетителях обрабатывается гостиницей в виде компьютерной информации. При заселении гостю требуется назвать свои данные ФИО, паспорт, место прописки, мобильный телефон все эти данные считаются персональными и согласно ФЗ №152 «О защите персональных данных» не подлежат разглашению, под угрозой санкций, применяемых к гостинице. Однако нередки случаи кражи таких данных, как ни странно, базы данных продаются в интернете и на них существует большой спрос. Задача гостиницы предотвратить несанкционированный доступ к этим данным, обеспечить максимальную информационную безопасность [30].

Согласно принципам хранения информации она должна быть конфиденциальна, целостна и доступна. Для этого на предприятиях устанавливается контроль за информацией [4].

Существует 3 вида контроля за состоянием информации на предприятии:

1. Административный контроль – Этот вид контроля включает государственные нормативные акты, принятую политику предприятия по безопасности, дисциплинарные меры к сотрудникам.

2. Логический контроль – это контроль информации на уровне средств управления, сюда входят пароли, межсетевые экраны, специальное защитное ПО.

3. Физический контроль – запрет использованию контрольных панелей и компьютеров лицам, не имеющим права на это, предотвращение физического проникновения [14].

Сбор персональных данных начинается, когда гость находится ещё на стадии бронирования. Важно отметить, что при бронировании через посредников ответственность за утечку со стороны агентов гостиница не несет. За защиту данных на сайте отвечает сертификат безопасности SSL, он создает безопасное соединение с шифрованием данных с созданием частного аутентифицированного канала, который обеспечивает надежную передачу данных от браузера к серверу.

При бронировании через сайт гостиницы клиент может предоставить платежные данные, утечка которых недопустима ни при каком раскладе. Для защиты платежных данных следует использовать одобренный стандарт безопасности Payment Card Industry Data Security Standard (PCI DSS) данный стандарт включает в себя 12 требований безопасности в области информации [9].

Сертификаты безопасности это один из способов защиты информации, они бывают следующих типов: организационные, аппаратные, программные и программно-аппаратные. Сертификаты относятся к программным способам защиты. Помимо них к программным относятся Антивирусы, Системы криптографии, Решения DLP, Межсетевые экраны, Решения SIEM [16].

Наиболее безопасными считаются IPC технологии, работающие по принципу DLP. Они представляют собой программно-аппаратный комплекс,

осуществляющий фильтрацию информации в обе стороны. Основной задачей которого является предотвращение утечек. Практика показывает, что более 70% утечек происходят по причине человеческого фактора, IPC системы предотвращают подавляющее большинство как ненамеренных утечек, так и проникновения со злым умыслом.

Дополнительные задачи систем класса IPC

- предотвращение передачи вовне не только конфиденциальной, но и другой нежелательной информации (обидных выражений, спама, эротики, излишних объёмов данных и т.п.);
- предотвращение передачи нежелательной информации не только изнутри наружу, но и снаружи внутрь информационной системы организации;
- предотвращение использования работниками Интернет-ресурсов и ресурсов сети в личных целях;
- защита от спама;
- защита от вирусов;
- оптимизация загрузки каналов, уменьшения нецелевого трафика;
- учет рабочего времени и присутствия на рабочем месте;
- отслеживание благонадёжности сотрудников, их политических взглядов, убеждений, сбор компромата;
- архивирование информации на случай случайного удаления или порчи оригинала;
- защита от случайного или намеренного нарушения внутренних нормативов;
- обеспечение соответствия стандартов в области информационной безопасности и действующего Законодательства.

IPC системы фильтруют входящие и выходящие данные, существует несколько методов работы таких систем [14].

Самый простой метод контроля — поиск в потоке данных некоторой последовательности символов. Иногда запрещенную последовательность

символов называют «стоп-выражением», но в более общем случае она может быть представлена не словом, а произвольным набором символов, например, определенной меткой. Если система настроена только на одно слово, то результат её работы — определение 100%-го совпадения, т.е. метод можно отнести к детерминистским. Однако чаще поиск определенной последовательности символов все же применяют при анализе текста. В подавляющем большинстве случаев сигнатурные системы настроены на поиск нескольких слов и частоту встречаемости терминов.

Метки. Суть этого метода заключается в расстановке специальных «меток» внутри файлов, содержащих конфиденциальную информацию. С одной стороны, такой метод дает стабильные и максимально точные сведения для DLP-системы, с другой стороны требуется много довольно сильных изменений в инфраструктуре сети. У лидеров DLP- и IPC-рынка реализация данного метода не встречается, поэтому рассматривать её подробно не имеет особого смысла. Можно лишь заметить, что, несмотря на явное достоинство «меток» — качество детектирования, есть множество существенных недостатков: от необходимости значительной перестройки инфраструктуры внутри сети до введения множества новых правил и форматов файлов для пользователей. Фактически внедрение такой технологии превращается во внедрение упрощенной системы документооборота.

Цифровые отпечатки. Суть данного принципа заключается в создании у системы определенных шаблонов защищенной информации, которому задается процент соответствия, при превышении порогового значения информация не проникает вовне

Есть еще ряд методов: метод «масок»; метод «карантина»; лингвистический «метод» [32].

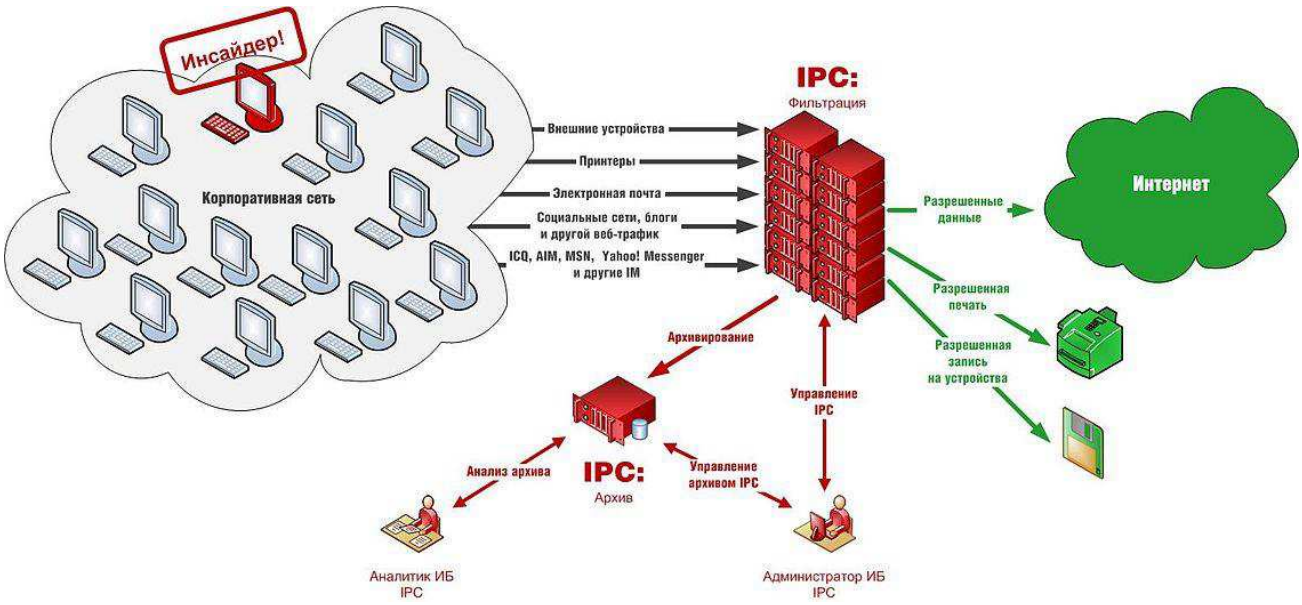


Рисунок 10 – Схема работы IPC системы

IPC система устанавливается на сервере, на серверах гостиницы содержатся рабочие базы данных, они являются управляющими компьютерами в локальных сетях, отвечают за wi-fi, соединение всех рабочих компьютеров-клиентов и прочее. Такие компьютеры имеют наибольший доступ ко всей сети гостиницы, при должном умении, знаниях злоумышленник может нанести гостинице большой ущерб, из этого следует, что помещение, где находятся сервера, должно располагаться не на зоне интенсивного движения, защищаться сигнализацией и видеокамерами [18].

В большинстве случаев, для обработки персональных данных о клиентах используются специальные программы – автоматизированные системы управления. Бесспорно такие программы упрощают работу персонала, позволяют видеть журнал событий и составлять автоматизированные отчеты, но зачастую эти программы настраиваются недостаточно тонко и могут быть уязвимы к проникновениям как извне с использованием удаленного доступа, так и за счет ошибочных или злонамеренных действий персонала. Такие программы позволяют присваивать разным пользователям различный уровень доступа. Для минимизации рисков рекомендуется составление матриц с различным уровнем доступа для разных групп пользователей.

Для оценки рисков несанкционированного доступа может использоваться как специальное программное обеспечение, так и так называемые «белые хакеры» в задачи которых входит поиск уязвимостей в системе, с целью их закрытия.

Однако установка ICP систем и невозможность получения удаленного доступа извне никак не оберегают систему от проникновения изнутри. Для предотвращения таких проникновений на предприятии вводится ряд организационных мер:

- разработка и внедрение инструкций пользователей и администраторов;
- безопасности;
- учет всех носителей электронной и иной информации;
- подписание договоров о неразглашении;
- составление инструкций по технологическому порядку обработки данных;
- составление регламента информационной безопасности;
- составление актов об установке средств защиты информации;
- установление пропускного режима и охраны

Персонал должен быть осведомлен о правилах работы с техническими средствами и банальной «культурой использования», так недопустимо при покидании рабочего места оставлять незавершенные сеансы на компьютерах, скачивать файлы из интернета на рабочий компьютер, переходить по подозрительным ссылкам из электронных сообщений и прочее.

Помимо таких действий руководству следует следить за тем, чтобы на компьютерах не было портов для подключения внешних накопителей, во избежание краж информации.

Для минимизации рисков нарушения информационной безопасности организации рекомендуется разработать политику информационной

безопасности, которая представляет собой перечень правил для различных областей деятельности организации.

Политика безопасности предполагает, в частности, четкое распределение функциональных обязанностей между администраторами сети, специалистами по информационной безопасности, руководителем информационного отдела и т.д., она должна предусматривать непрерывность контроля за системами защиты информации, персональную ответственность специалистов, оперативность в принятии управленческих решений в зависимости от конкретной складывающейся ситуации, нацеленность руководства и персонала гостиничного комплекса на обеспечение информационной безопасности [27].

Также следует отметить, что в подавляющем большинстве гостиниц имеется wi-fi, как рабочий, так и для гостей. Он является еще одной уязвимой точкой в информационной сети гостиницы. Сети обязательно быть разделены. Недопустимо давать гостям доступ к рабочему wi-fi, так и подключать рабочие компьютеры к гостевой сети. Гостевая сеть должна иметь аутентификацию по номеру или мобильному телефону и это не прихоть гостиниц, а требование, которое должно соблюдаться согласно Постановлениям Правительства РФ №758 и № 801 и ФЗ № 97 «Об информации, информационных технологиях и о защите информации». Делается это с целью защиты сетей от мошенников и злоумышленников. Также роутеры желательно должны обладать новыми протоколами безопасности WPA3, он обеспечивает более надежное шифрование паролей и повышенную защиту от брутфорс-атак

Выводы по 1 главе

1. Технические средства являются частью информационных технологий и находятся в ведении IT-департамента и службы безопасности. Технические средства используются для автоматизации процессов и исключения человеческого фактора.

2. Основными угрозами в гостиницы являются: Пожароопасные факторы, криминогенные факторы, техногенные факторы, природные факторы.

3. Выделено несколько основных систем технических средств: система охранно-пожарной сигнализации, система контроля и управления доступом, система противопожарной безопасности, система видеонаблюдения и система защиты информации.

4. СКУД – механизм отслеживания входа и выхода, отвечает за санкционированный доступ в помещения гостиницы

5. Система ОПС предназначена для оповещения о фактах несанкционированного доступа и пожароопасных ситуаций.

6. Система противопожарной безопасности направлена на обнаружение, оповещение, тушение и предотвращение пожара.

7. Система видеонаблюдения направлена на круглосуточный контроль, за территорией гостиничного предприятия, выявление действий преступного характера.

8. Вышеперечисленные системы имеют возможность интеграции в единую автоматизированную систему управления путем использования специализированного софта и аппаратно-программных модулей.

9. Система защиты информации направлена на предотвращение хакерских атак на сервера и компьютеры гостиничного предприятия.

Заключение

Безопасность – одна из основных потребностей человека. Уровень безопасности в гостинице должен удовлетворять ожиданиям клиентов в целях повышения комфорта пребывания в гостинице.

Гостиницы со своей инфраструктурой, специфической жизнью, большим потоком людей, грузов и материальных ценностей требуют особых мер по обеспечению безопасности.

В современном мире поддерживать уровень безопасности человеку помогают информационные технологии. С развитием технических средств благодаря специализированному программному обеспечению стали доступны возможности интеграции позволяющие сократить количество трудозатрат со стороны человека.

Комплексный подход к организации безопасности гостиничного хозяйства требует умелого управления. Это связано с тем, что в гостиницах применяются различные технические средства и автоматизированные системы обеспечения безопасности.

В дипломной работе в качестве теоретической основы были рассмотрены аспекты использования информационных технологий и технических средств, в частности; основные внешние угрозы для гостиничного предприятия; основы использования СКУД, ОПС, видеонаблюдения, систем защиты информации и интеграция систем защиты в автоматизированные системы управления.

Проведен общий анализ гостиничного предприятия «Мемфис» в городе Красноярск. Изучены особенности использования информационных технологий в системе безопасности гостиницы.

Предложен комплекс мер для более эффективного использования технических средств в составе информационных технологий в системе безопасности гостиничного предприятия.

Результатами внедрения данных мер должны быть:

- Повышение уровня комфорта гостей во время пребывания в гостинице.
- Повышение эффективности труда персонала, за счет автоматизации ряда процессов.
- Экономический эффект – предложенные меры экономически окупятся спустя 2,5 года, далее гостиница будет получать дивиденды за счет внедрения предложенных мер

Список использованных источников

1. Автоматическая система дымоудаления, обслуживание, особенности монтажа // Сигнализации. Все для защиты дома. – 2017 – URL: https://signalkaman.ru/zamena/avtomaticheskaya-sistema-dymoudaleniya-obsluzhivanie-osobennosti-montazha.html (дата обращения: 29.04.2022)
2. Алексеева, Е.Ю. DLP-Системы. Методология и продукты/ Е.Ю. Алексеева, А.А. Бутин // Журнал Иркутского государственного университета путей сообщения – 2016 - №17 – 23-28 с.
3. Бурькова, Е. В. Системы охранно-пожарной сигнализации : учебное пособие / Е. В. Бурькова. — Оренбург : ОГУ, 2019. — 134 с. — ISBN 978-5-7410-2303-7.
4. Василенко К.А. Проблематика информационной безопасности в компьютерных сетях: сетевые протоколы и их особенности/ К.А. Василенко, В.А. Щетилин // Журнал Владивостокского государственного университета экономики и сервиса – 2020 - №2 – 78-82 с.
5. Введение во взаимную аутентификацию // PCnews – статьи из мира технологий – 2019 – URL: https://pcnews.ru/blogs/vvedenie_vo_vzaimnuu_autentifikaciu_servisov_na_java_c_tlsssl-959222.html#gsc.tab=0 (дата обращения: 13.05.2022).
6. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний = Access control units and systems. Classification. General technical requirements. Test methods: национальный стандарт Российской Федерации: издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2008 г. N 430-ст
7. ГОСТ Р 54831-2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний = Control access systems. Controlled barrier units. General

technical requirements. Test methods: национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 13 декабря 2011 г. N 1223-ст

8. Дьячков Д.И. Особенности программного обеспечения гостиничных СКУД/ Д.И. Дьячков // Журнал Петерсофт – 2017 - №3 – 8-10 с.

9. Ерохин В.В. Верификация информационных систем коммерческого банка / В.В. Ерохин, Е.В. Елисеева // Журнал Брянского государственного университета – 2017 - №9 – 20-23 с.

10. Интеграция СВН, СКУД и ОПС // Корус АКС – системный интегратор – 2018 – URL: http://www.quorus.ru/pages/integratsiya-svn-skud-i-ops-ohranno-pojarnaya-signalizatsiya (дата обращения 03.05.2022).

11. Костарев, С. Н. Пожарная автоматика, управление и связь: учебное пособие / С. Н. Костарев. — Пермь: ПНИПУ, 2017. — 123 с. — ISBN 978-5-398-01731-1.

12. Кучеренко, В. Л. Менеджмент безопасности гостиничного предприятия: учебное пособие / В. Л. Кучеренко. — Санкт-Петербург: Троицкий мост, 2013. — 160 с. — ISBN 978-5-4377-0021-1.

13. Лазарева Л.А. Обеспечение безопасности в гостиницах: учебно-методическое пособие для практических занятий и самостоятельной работы / Л.А. Лазарева; ФГБОУ ВО РГУПС. – Ростов н/Д, 2017. – 47 с.

14. Минакова Н.Н. Методы и средства защиты информации в коммерческой организации: монография / Н.Н. Минакова, В.В. Поляков, П.В. Плетнев; Барнаул: Изд-во «Новый формат», 2016. – 158 с.

15. Материалы тридцатой международной научно-технической конференции "Системы безопасности – 2021" / Под общей редакцией д-ра техн. наук, профессора Топольского Н.Г. – М.: Академия ГПС МЧС России, 2021. 547 с.

16. Махмадиев Ш.Х. DLP-система как основа защиты компьютерной информации / Ш.Х. Махмадиев // Системы защиты информации: тезисы

докл. Всерос. Конф. (Воронеж, 14-16 апр. 2014 г.) – Воронеж, 2014 – 124-125с.

17. Махов, С. Ю. Безопасность в туризме : учебно-методическое пособие / С. Ю. Махов. — Орел : МАБИВ, 2020. — 118 с. — ISBN 2413-6379.

18. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для вузов / С. Н. Никифоров. — 4-е изд., стер. — Санкт-Петербург : Лань, 2022. — 96 с. — ISBN 978-5-8114-9562-7.

19. Омельянчук А.Г. Интеграция СКУД и ОПС. Польза или вред? / А.Г. Омельянчук // Журнал Технологии защиты – 2012 - №6 – 59-16 с.

20. Петкевич К.А. Информационные технологии в государственном и муниципальном управлении / К.А. Петкевич // Журнал Балтийского федерального университета – 2020 - №64 – 60-62с.

21. Платежный шлюз Moneta.ru сертифицирован по стандарту PCI DSS // Hi-tech News – 2014 – URL: https://www.cnews.ru/news/news/platezhnyj_shlyuz_moneta.ru_sertifitsirovan (дата обращения: 29.05.2022).

22. Поликанин, А. Н. Технические средства охраны и видеонаблюдения. Системы видеонаблюдения и тепловизионного контроля: учебное пособие / А. Н. Поликанин. — Новосибирск: СГУГиТ, 2021. — 46 с. — ISBN 978-5-907320-92-5.

23. Постановление Правительства РФ от 18.11.2020 №1860 «Об утверждении Положения о классификации гостиниц»

24. Постановление Правительства РФ от 26.04.2022 N 758 "О внесении изменений в некоторые акты Правительства Российской Федерации"

25. Прохорова, О. В. Информационная безопасность и защита информации: учебник для спо / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с. — ISBN 978-5-8114-8924-4.

26. Технические средства информатизации // Образовательный портал School -2020 -URL: https://www.sites.google.com/site/informatikadzabasova/tehniceskie-sredstva-informatizacii (дата обращения: 15.05.2022).

27. Топольник В.Г, Моделировании организации работы службы безопасности гостиницы средствами IDEF0 / Топольник В.Г, Цехмистер // Журнал теория и практика современной науки – 2016. - №7. – с 324 - 333

28. СП 3.13130.2009 Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре. Требования пожарной безопасности: дата введения 05.01.2009.

29. СП 10.13130.2020 Системы противопожарной защиты. Внутренний противопожарный водопровод. Нормы и правила проектирования: дата введения: 27.01.2021

30. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ: [принят Государственной думой 8 июля 2006 года: одобрен Советом Федерации 14 июля 2006 года]. – Москва: Проспект; Санкт-Петербург: Кодекс, 2017. – 158 с. – ISBN 978-5-392-26365-3.

31. Черевичко, Т. В. Гостиничный сервис : учебное пособие / Т. В. Черевичко, М. С. Отнюкова. — Москва : ФЛИНТА, 2021. — 179 с. — ISBN 978-5-9765-4964-7.

32. Information protection and control // TadViser Государство.Бизнес.Технологии – 2019 – URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:IPC (дата обращения: 2.06.2022)

Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт торговли и сферы услуг
Кафедра гостиничного дела

УТВЕРЖДАЮ
Заведующий кафедрой
_____ М. Д. Батраев
подпись инициалы, фамилия
«14» 06 2022 г.

БАКАЛАВРСКАЯ РАБОТА

43.03.03 Гостиничное дело
код и наименование направления подготовки

43.03.03.02.01 Ресторанное дело
код и наименование профиля подготовки

Особенности использования информационных технологий в обеспечении безопасности гостиницы на примере гостиницы «Берега»
тема

Руководитель 10.06.22 доцент, канд.техн.наук Т. Н. Сафронова
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник 09.06.2022 Р. Р. Ризванов
подпись, дата инициалы, фамилия

Нормоконтролер 10.06.22 Т. Н. Сафронова
подпись, дата инициалы, фамилия

Красноярск 2022