

Государственное автономное профессиональное образовательное
учреждение Калужской области
«Калужский технический колледж»
ГАПОУ КО «КТК»

Дипломный проект выполнен
и защищен с оценкой _____
Председатель ГЭК _____
«_____» _____ 2022г.

Допущен к защите
Зам. директора по УТР
_____ И.М. Ковалева
«_____» _____ 2022г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(ДИПЛОМНАЯ РАБОТА)

НА ТЕМУ: «ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ КОМПЛЕКСНОЙ
СИСТЕМЫ ЗАЩИТЫ РЕСТОРАНА «Макдоналдс»

Студента: Симоненкова Вадима Дмитриевича

Специальность: Организация и технология защиты информации

Группа: 4 ОТЗИ

Руководитель дипломного проекта _____ В.В. Голиков

г. Калуга, 2022г.

Содержание

Введение.....	3
Глава 1. Анализ теоретических основ организации ресторана.....	6
1.1. Анализ исследуемого ресторана «Макдоналдс».....	6
1.2. Организационная структура.....	8
1.3. Нормативные документы для работы ресторана «Макдоналдс».....	13
1.3.1. Межгосударственные и национальные документы.....	13
1.3.2. Санитарно-эпидемиологические требования.....	15
1.3.3. Правила охраны труда в общественном питании.....	15
1.3.4. Технические регламенты.....	16
1.4. Анализ угроз для современной организации.....	16
1.5. Анализ рисков и угроз для ресторана «Макдоналдс».....	21
1.6. Матрица безопасности ресторана «Макдоналдс».....	23
1.7. Описание информационной среды ресторана «Макдоналдс».....	26
Глава 2. Реализация комплексной системы защиты.....	29
2.1. Выбор средств физической защиты ресторана «Макдоналдс».....	29
2.3. Выбор средств защиты информационно-коммуникационного оборудования ресторана «Макдоналдс».....	57
2.4. Применяемые охранные и пожарно-охранные средства.....	61
2.5. Рекомендации по усовершенствованию комплексной системы безопасности ресторана быстрого питания.....	63
Заключение.....	65
Список источников и литературы.....	67

ВВЕДЕНИЕ

Информация – очень важный ресурс в современном мире, ровно как и остальные ресурсы информация имеет свою ценность, каждый день мы обрабатываем огромное её количество, именно поэтому информацию нельзя оставлять без внимания, так как её используют не только добросовестные люди, но и злоумышленники, их цели могут быть разными, но все они сводятся именно к негативному воздействию на информацию. Именно поэтому в современном мире имеет место быть тенденция роста систем защиты информации.

Абсолютно любое предприятие или организация имеет информацию, которая не должна быть доступна третьим лицам, это могут быть чертежи, бухгалтерская отчетность и многое другое, такую информацию называют конфиденциальной и её необходимо как следует защищать, для этого нам необходима комплексная система защиты информации. Комплексная система защиты информации (КСЗИ) – совокупность организационных и инженерно-технических мероприятий, которые направлены на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа.

КСЗИ является глобальной концепцией безопасности и основой для безопасности инфраструктуры предприятия в целом. Благодаря грамотной постройке КСЗИ можно избежать несанкционированного доступа со стороны злоумышленников, что в дальнейшем поможет сохранить предприятие на рынке и способствовать дальнейшему его продвижению. Конечной целью создания комплексной защиты информации является полное препятствование попыткам несанкционированного доступа к конфиденциальной информации предприятия.

Используя различные методы и средства информационной комплексной защиты, невозможно достичь абсолютно идеальной безопасности организации. Средств защиты не бывает слишком много,

однако с ростом уровня защищенности той или иной части возникают и, как правило, определенные неудобства в ее использовании, ограничения и трудности для сотрудников и клиентов. Поэтому, часто необходимо выбрать оптимальный вариант защиты, который бы не создавал больших трудностей в пользовании и одновременно обеспечивал достойный уровень защиты организации и данных. Подчас создание такого оптимального решения безопасности является очень сложным.

Актуальность темы данного исследования определяется в том, что антикриминальная и антитеррористическая безопасность представляет собой один из наиболее важных и ответственных элементов обеспечения безопасности любого объекта, особенно если это касается мест массового скопления людей. Безопасности гостей и сотрудников ресторана необходимо уделять повышенное внимание.

Объектом исследования данной работы является комплексная безопасность в ресторане Макдоналдс.

Предметом исследования выступают методы и средства, которые позволяют обеспечить комплексную защиту ресторана Макдоналдс.

Целью данной работы является проектирование и реализация комплексной системы защиты ресторана «Макдоналдс». Важной составляющей работы является рассмотрение существующих и применяемых методов и средств комплексной защиты, а именно основных вопросов и понятий защиты и безопасности, видов угроз безопасности, не только программных, физических, но и правовых методов и средств обеспечения комплексной защиты.

Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать необходимость организации комплексной защиты;
- исследовать внешние и внутренние угрозы объекта защиты;

- оценить перспективные решения в сфере обеспечения комплексной безопасности;
- изучить существующие конкретные средства и методы комплексной защиты.

Для выполнения всех поставленных в работе целей и задач будут использоваться методы анализа научной литературы, метод синтеза, сравнения, сбора и выборки.

Данная выпускная квалификационная работа состоит из двух глав. Первая глава теоретическая, где рассматриваются: цели и задачи организации комплексной защиты ресторана Макдоналдс, цели и средства по обеспечению информационной безопасности, анализ существующего организационно–правового механизма защиты.

Вторая глава аналитическая, где проводится: анализ структуры средств и методов обеспечения системы комплексной безопасности ресторана быстрого питания, рекомендации по оптимизации комплексной системы защиты обеспечения безопасности при функционировании ресторана.

При написании выпускной квалификационной работы в качестве теоретической базы использовался широкий круг научной литературы.

ГЛАВА 1. АНАЛИЗ ТЕОРЕТИЧЕСКИХ ОСНОВ ПРЕДПРИЯТИЯ

1.1. Анализ исследуемого предприятия

Российский рынок общественного питания растёт стабильными темпами. Возможностью получать значительные прибыли привлекает в этот бизнес большое количество инвесторов, как отечественных, так и зарубежных. Наметилась четкая тенденция - от года к году россияне меньше питаются дома и чаще посещают рестораны, кафе, бары.

Значительное увеличение количества предприятий общепита, по мнению экспертов, стало возможным благодаря увеличению покупательной способности и росту деловой активности населения, вызванной ускорением ритма жизни, вынуждающей наиболее платежеспособную часть работоспособных граждан питаться вне дома. Согласно экспертным наблюдениям, городские жители начинают периодически посещать предприятия общественного питания, имея доход от 30000 руб. в месяц. Регулярными клиентами подобных заведений становятся обладатели ежемесячного дохода от 50000 – 70000 руб. в месяц.

Посещение ресторана или кафе уже давно перестало быть атрибутом праздника или исключительного события для большинства населения.

Сектор общественного питания удовлетворяет очень сложный комплекс потребностей — от простого утоления чувства голода и жажды до имиджевых и статусных притязаний. Поэтому характерной чертой нынешнего состояния рынка является его неоднородность и разносторонний охват практически всех целевых аудиторий потребителей: по уровню доходов, по возрасту, полу, по социальному статусу и интересам.

Особенно быстрые темпы роста количества посетителей отмечают среди демократичных предприятий – заведений класса «casual», «фаст-фуд», пиццерий. Они пользуются популярностью более чем у половины населения за доступность и быстрое обслуживание.

Быстрый рост современного рынка общественного питания во многом обусловлен развитием фаст-фуда. По оценкам экспертов годовой прирост

этого сектора уже в течение нескольких лет составляет до 25 %. Фаст-фуд становится все более востребованным: если раньше основная масса людей питалась в рабочее время на работе бутербродами и т.п., то сейчас многие предпочитают куда-то выйти на обед.

Развитие фаст-фуда происходит не только за счет количества точек. Расширяется меню, все больше появляется блюд, рассчитанных на потребителей с небольшими доходами. Большинство заведений по-прежнему ориентируются на сумму разовой покупки около 300 – 500 руб. Основные концептуальные бренды сгруппированы по реализуемым товарным группам: гамбургеры, пицца, цыпленок, бифштексы, дары моря, национальные блюда.

В связи с высокой популярностью ресторанов быстрого питания Макдоналдс, всё более серьезно встает вопрос организации их комплексной системы защиты. Необходимо организовывать систему таким образом, чтобы она позволяла максимально снизить риски как для сотрудников организации, так и для её клиентов.

Комплекс мероприятий по безопасности ресторанов быстрого питания включает в себя несколько инструментов:

- регулярное проведение организационных мероприятий, направленных на обеспечение максимально эффективной защиты от возможности совершения криминальных и террористических актов. Это различные тренинги, памятки, практические игры для сотрудников. Необходимо как можно чаще напоминать людям, что наша безопасность в наших руках, обращать внимание на объемные вещи, сумки, коляски, рюкзаки, емкости для жидкости;
- использование информационно-коммуникационных технологий. Это система видеомониторинга, система оповещения, беспроводная связь между сотрудниками;
- оборудование ресторанов всеми необходимыми инженерно-техническими устройствами. К ним относятся специализированные инженерные средства, которые могут препятствовать несанкционированному

доступу на объект;

- обеспечение полноценного контроля в едином информационном пространстве, причем обеспечение его в режиме реального времени для постоянного мониторинга обстановки.

Любая кризисная ситуация непредсказуема, каждый раз это что-то новое, нельзя быть уверенным, что система безопасности готова ко всему, это ошибочное мнение большинства. Эффективные методы подготовки сотрудников могут лишь помочь, если кризисная ситуация настигла. Нужно вырабатывать в сотрудниках схему действий, постоянно напоминать о первоочередных мерах, ведь ситуации зачастую бывают внезапными и чреватыми быстро развивающимися последствиями. Главное – делиться информацией, оповещать все возможные инстанции о сложившейся ситуации, даже несколько секунд могут спасти кому-то жизнь, но и при этом нельзя забывать о своей жизни.

1.2. Организационная структура предприятия

Организационная структура — это состав, взаимосвязь самостоятельных управленческих подразделений и отдельных должностей.

В данной дипломной работе будет исследоваться и прорабатываться вопрос организации комплексной системы защиты одного ресторана компании «Макдоналдс».

Организационная структура сети ресторанов компании «Макдоналдс» представляет собой иерархическую модель. Рисунок 1.1

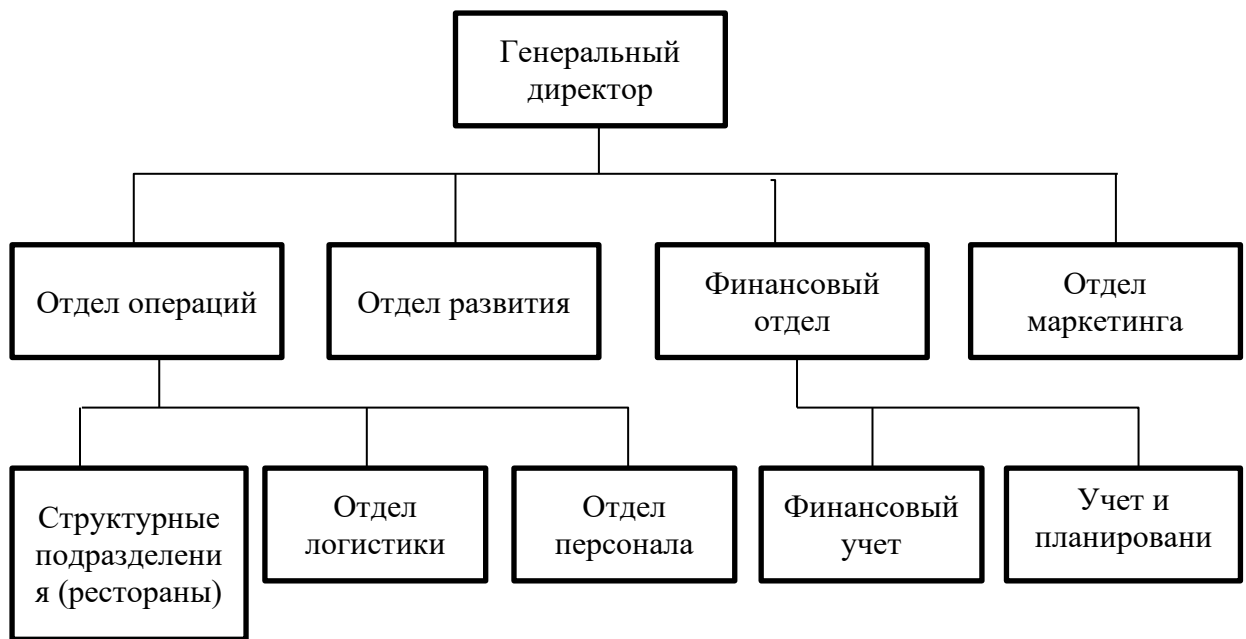


Рисунок 1.1. Организационная структура сети ресторанов

«Макдоналдс»»

Далее необходимо рассмотреть организационную структуру непосредственно ресторана, который рассматривается в данной дипломной работе. Рисунок 1.2.

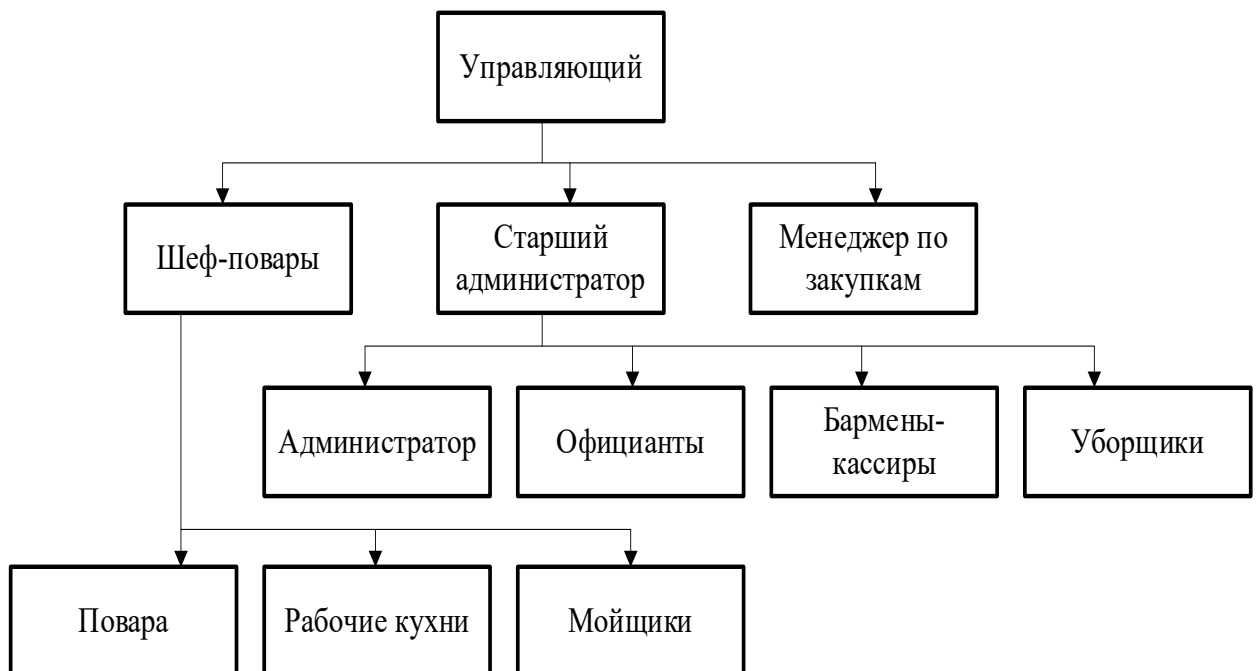


Рисунок 1.2. Организационная структура ресторана «Макдоналдс»

Организационная структура «Макдоналдс» – это иерархическая структура, а, следовательно, в системе управления идет чёткое разделение

труда, которое способствует появлению высококвалифицированных специалистов в каждом деле; строгой иерархии уровней управления, при которой действия нижестоящего звена управления контролируются вышестоящим и выработке единых для каждого вида деятельности правил, норм и стандартов.

В каждом ресторане есть управляющий. Круг его обязанностей состоит из следующих функций:

- Оформляет документы, необходимые для осуществления деятельности по оказанию услуг общественного питания;
- Осуществляет организацию, планирование и координацию деятельности ресторана;
- Осуществляет контроль над рациональным использованием материальных, финансовых и трудовых ресурсов, производит оценку качества обслуживания клиентов;
- Заключает договора поставки продовольственных товаров, контролирует сроки, ассортимент, количество и качество их поступления и реализации;
- Предоставляет отчетность о производственной деятельности, в том числе владельцу ресторана;
- Устанавливает служебные обязанности для подчиненных ему работников и принимает меры по обеспечению их исполнения;
- Принимает решения о назначении, перемещении и освобождения от занимаемых должностей работников ресторана, применяет меры поощрения отличившихся работников, налагает взыскания на нарушителей производственной и трудовой дисциплины.

Функции старшего администратора:

- Осуществляет контроль над рациональным оформлением зала, барных стоек, витрин, и т.д.;
- Принимает меры к предотвращению и ликвидации конфликтных

ситуаций;

- Рассматривает претензии, связанные с неудовлетворительным обслуживанием посетителей, и проводит соответствующие организационно-технические мероприятия;
- Контролирует соблюдение работниками организации трудовой и производственной дисциплины, правил и норм охраны труда, техники безопасности, требований производственной санитарии и гигиены;
- Информировывает руководство организации об имеющихся недостатках в обслуживании посетителей, принимает меры к их ликвидации;
- Выполняет отдельные служебные поручения своего непосредственного руководителя.

Функции шеф-повара:

- Осуществляет руководство производственно-хозяйственной деятельностью подразделения предприятия общественного питания;
- Направляет деятельность трудового коллектива на обеспечение ритмичного выпуска продукции собственного производства требуемого ассортимента и качества в соответствии с производственным заданием;
- Составляет заявки на необходимые продовольственные товары и сырье, обеспечивает их своевременное получение со склада, контролирует сроки, ассортимент, количество и качество их поступления в реализацию;
- Осуществляет постоянный контроль над технологией приготовления пищи, нормами закладки сырья и соблюдением работниками санитарных требований и правил личной гигиены;
- Контролирует правильную эксплуатацию оборудования и других основных средств;
- Контролирует соблюдение работниками правил и норм охраны труда и техники безопасности, санитарных требований и правил личной гигиены, производственной и трудовой дисциплины, правил внутреннего трудового распорядка.

Официанты выполняют следующие функции и задачи:

- Контроль за чистотой, состоянием и комплектностью приборов, посуды, скатертями и салфетками на закрепленных за официантом столами;
- Изучение меню, знание основных и сезонных блюд и напитков, предлагаемых гостям;
- Консультирование гостей ресторана об особенностях блюд и напитков, предлагаемых гостям;
- Прием заказов от клиента ресторана;
- Принятие мер, в рамках своей компетенции, по разрешению проблем, возникших у клиента;
- Создание атмосферы гостеприимства;
- Получение платы по счетам.

Функции, которые выполняет повар:

- Подготавливает основную продукцию, входящую в меню, и готовить обеды для персонала, строго соблюдая технологический процесс и согласно установленным рецептам;
- Соблюдать правила товарного соседства и ротации продуктов, контролировать сроки реализации продуктов;
- Отпускать готовые блюда строго по чекам;
- Поддерживать чистоту и порядок на кухне и на своем рабочем месте в соответствии с требованиями СЭС;
- Своевременно информировать администрацию об отсутствии продуктов, о неисправностях инвентаря, сантехники.

Мойщик посуды:

- Мойка столовой посуды с применением моющих средств в течение всего рабочего дня;
- Очистка тарелок и стаканов от пищевых отходов;
- Доставка чистой посуды на раздаточные столы;
- Содержание в чистоте и соблюдение правил эксплуатации

посудомоечной машины.

Уборщик:

- Производит уборку помещений ресторана;
- Вытирает пыль, подметает и моет полы, лестницы, окна, стены, плинтуса, потолки в помещениях ресторана;
- Расставляет урны для мусора, своевременно очищает и дезинфицирует их;
- Убирает и дезинфицирует туалеты и другие места общего пользования.

Каждый сотрудник ресторана быстрого питания «Макдоналдс» имеет возможность расти и развиваться. Даже самый простой работник, со временем может получить высокую должность, если будет качественно выполнять свои обязанности и отлично проходить все аттестации.

Вся полнота ответственности за обеспечение безопасности возлагается на руководителя и должностных лиц заведения.

1.3. Нормативные документы для работы предприятия общественного питания

Организация работы и качественное функционирование ресторана «Макдоналдс» невозможно без использования нормативно-правовых документов. Деятельность предприятия общественного питания, в том числе и ресторанов «Макдоналдс», строго регламентировано целым набором нормативных документов и стандартов.

1.3.1. Межгосударственные и национальные документы

Услуги общественного питания:

- ГОСТ 30389-2013 Предприятия общественного питания.

Классификация и общие требования;

- ГОСТ 30524-2013 Требования к персоналу;
- ГОСТ 31984-2012 Услуги общественного питания. Общие требования;

- ГОСТ 31985-2013 Термины и определения;
- ГОСТ 31989-2012 Общие требования к заготовочным предприятиям общественного питания;
- ГОСТ 32691-2014 Порядок разработки фирменных и новых блюд и изделий на предприятиях общественного питания;
- ГОСТ 32692-2014 Общие требования к методам и формам обслуживания на предприятиях общественного питания;
- ГОСТ Р 55323-2012 Идентификация продукции общественного питания. Общие положения;
- ГОСТ Р 55889-2013 Система менеджмента безопасности продукции общественного питания. Рекомендации по применению;
- ГОСТ Р ИСО 22000-2007 для индустрии питания Безопасность бытовых и аналогичных электрических приборов;
- ГОСТ 27570.42-92 Частные требования к электрическим тепловым шкафам для предприятий общественного питания;
- ГОСТ 27570.53-95 Частные требования к электрическим кухонным машинам для предприятий общественного питания;
- ГОСТ ИЕС 60335-2-15-2014 Частные требования к приборам для нагрева жидкостей;
- ГОСТ ИЕС 60335-2-25-2014 Частные требования к микроволновым печам, включая комбинированные микроволновые печи;
- ГОСТ ИЕС 60335-2-38-2013 Частные требования к электрическим аппаратам контактной обработки продуктов с одной и двумя греющими поверхностями для предприятий общественного питания;
- ГОСТ ИЕС 60335-2-39-2013 Частные требования к электрическим универсальным сковородам для предприятий общественного питания;
- ГОСТ ИЕС 60335-2-48-2013 Частные требования к электрическим грилям и тостерам для предприятий общественного питания;
- ГОСТ ИЕС 60335-2-62-2013 Частные требования к

ополаскивающим ваннам с электрическим нагревом для предприятий общественного питания;

- ГОСТ ИЕС 60335-2-75-2013 Частные требования к дозирующим устройствам и торговым автоматам для предприятий общественного питания;

- ГОСТ Р 52161.2.36-2012 Частные требования к электрическим кухонным плитам, шкафам и конфоркам для предприятий общественного питания;

Оборудование технологическое

- ГОСТ 16318-77 Оборудование технологическое для предприятий торговли и общественного питания. Термины и определения;

- Пожарная безопасность. Общие требования;

- ГОСТ 30494-2011 Здания жилые и общественные. Параметры микроклимата в помещениях;

- ГОСТ 30826-2014 Стекло многослойное. Технические условия;

- ГОСТ 32144-2013 Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения.

1.3.2. Санитарно-эпидемиологические требования

- СП 2.3.6.1079-01. 2.3.6 Организации общественного питания. Санитарно-эпидемиологические требования к организациям общественного питания, изготовлению и оборотоспособности в них пищевых продуктов и продовольственного сырья. Санитарно-эпидемиологические правила;

- СанПиН 2.3.2.1293-03 Гигиенические требования по применению пищевых добавок;

- СанПиН 2.3.2.1324-03 Гигиенические требования к срокам годности и условиям хранения пищевых продуктов;

1.3.3. Правила охраны труда в общественном питании

- ПОТ Р М-011-2000 Межотраслевые правила по охране труда в

общественном питании;

- СП 31-110-2003 Проектирование и монтаж электроустановок жилых и общественных зданий;
- СП 3.13130.2009 Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре. Требования пожарной безопасности;
- СП 5.13130.2009 Системы противопожарной защиты. Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования;
- СП 30.13330.2012 Внутренний водопровод и канализация зданий;
- СП 52.13330.2011 Естественное и искусственное освещение;
- ПУЭ (6-е и 7-е издание) Правила устройства электроустановок;
- СНиП 2.04.05-91* Отопление, вентиляция и кондиционирование;
- СНиП 21-01-97 Пожарная безопасность зданий и сооружений;

1.3.4. Технические регламенты и правила

- ТР ТС 021/2011 Технический регламент Таможенного союза «О безопасности пищевой продукции»;
- Федеральный закон от 30 декабря 2009 г. № 384-ФЗ;
- Технический регламент о безопасности зданий и сооружений;
- Федеральный закон от 22 июля 2008 г. № 123-ФЗ;
- Технический регламент о требованиях пожарной безопасности;
- Постановление Правительства РФ от 25 апреля 2012 г. № 390 «О противопожарном режиме»;
- Правила противопожарного режима в Российской Федерации.

1.4. Анализ угроз для современной организации

Для любого современного предприятия существует множество угроз, и сейчас мы их рассмотрим.

Угроза безопасности организации - это:

- Совокупность факторов, воздействий внешней и внутренней среды предприятия, которые нацелены на незаконное или злостное воспрепятствование, или затруднение его функционирования в соответствии с уставными, долгосрочными и краткосрочными целями и задачами, а также на отчуждение результатов его деятельности;

- Потенциальные или реальные действия физических или юридических лиц, нарушающее состояние защищенности субъекта предпринимательской деятельности и способные привести к ее прекращению, либо к экономическим и другим потерям.

Угрозы бывают внутренние и внешние, преднамеренные и непреднамеренные:

К внутренним угрозам относятся - действия или бездействия (в том числе умышленные и неумышленные) сотрудников организации, противоречащие интересам его коммерческой деятельности, следствием которых могут быть нанесение экономического ущерба компании, утечка или утрата информационных ресурсов в том числе сведений, составляющих коммерческую тайну или конфиденциальную информацию.

К внешним угрозам относятся - стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т. п.); кибератаки; преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Преднамеренные угрозы

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

- физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

- отключение или вывод из строя подсистем обеспечения

функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

- действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);

- внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

- вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;

- применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;

- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);

- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

- хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);

- несанкционированное копирование носителей информации;

- хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

- чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты)

или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;

- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя ("маскарад");

- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;

- вскрытие шифров криптозащиты информации;

- внедрение аппаратных спецвложений, программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

- незаконное подключение к линиям связи с целью работы "между строк", с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

- незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений. Чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

Чаще всего для достижения поставленной цели злоумышленник

использует не один, а некоторую совокупность из перечисленных выше путей.

Непреднамеренные угрозы

Основные непреднамеренные искусственные угрозы КС (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
- неправомерное отключение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходом ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- заражение компьютера вирусами;
- неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек,

пропусков и т.п.);

- проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

1.5. Анализ рисков и угроз для ресторана «Макдоналдс»

При проведении анализа деятельности ресторана «Макдоналдс» с точки зрения организации комплексной системы безопасности критические риски выглядят следующим образом:

- возможность изъятия информации при ведении управленческого учета;
- недобросовестность сотрудников;
- возможность проникновения посторонних лиц;
- повышенная вероятность пожара;
- конфликтные ситуации;
- кражи на бытовом уровне;
- порча имущества ресторана;
- различные махинации с кассой;
- нарушения технологии приготовления блюд.

Возможность изъятия информации при ведении управленческого учета – это риск, при котором возможна потеря или разглашение

коммерческой тайны административным составом ресторана. Разглашение может быть как преднамеренным, так и непреднамеренным. В современных ресторанах устанавливаются компьютеры, на которых управляющие ведут учет. Именно они оказываются наиболее уязвимой точкой хранения коммерческой информации. Зачастую, сами того не понимая, пользователи этих компьютеров становятся причиной утечки важных данных. Для защиты таких ПК использует комплекс мер, позволяющий заблокировать наиболее вероятные пути утечки информации, такие как: возможность подключать съемные носители данных; выгрузку информации в интернет; случайную или намеренную отправку данных по электронной почте и другие.

Такие системы позволяют вести наблюдение за всеми действиями пользователя на компьютере и записывать их в журнал, что дает возможность успешно провести расследование нарушения и определить виновного.

Недобросовестность сотрудников – необходимо учитывать, что сотрудники являются наиболее уязвимым звеном при организации комплексной системы безопасности. От их действий во многом зависит общий успех деятельности предприятия.

Возможность проникновения посторонних лиц – осуществление несанкционированного доступа в зоны, предназначенные для персонала ресторана, а также проникновение в помещение предприятия во время отсутствия работников, например, в ночное время суток.

Повышенная вероятность пожара – для любого типа ресторана, это одна из наиболее вероятных угроз возникновения нештатной ситуации. От того, насколько грамотно будет организована защита от данного вида угрозы, может зависеть жизнь и здоровье сотрудников ресторана и посетителей. Основные причины пожара в ресторанах: нарушение правил эксплуатации кухонного оборудования, неисправные электропроводка и электрооборудование, человеческий фактор (неосторожное обращение с огнем).

Конфликтные ситуации, кражи на бытовом уровне, порча имущества ресторана, различные махинации с кассой, нарушения технологии приготовления блюд – всё это более мелкие виды угроз и рисков, но именно они могут нанести непоправимый ущерб репутации, комфорту посетителей, атмосфере уюта и доброжелательности.

Во времена жесткой конкуренции каждое предприятие ищет способы минимизировать свои затраты и повысить эффективность работы. Эффективность ресторанного бизнеса, как никакого другого, зависит от эффективности и добросовестности сотрудников.

Анализ рисков позволяет выделить в ресторане «Макдоналдс» наиболее критические зоны:

- основной вход;
- бар-касса, зона раздачи;
- прием товара;
- кабинет администрации;
- серверная;
- кухня;
- дверь холл/кухня;
- комната отдыха;
- холл ресторана.

1.6. Матрица безопасности ресторана «Макдоналдс»

Для построения матрицы безопасности, необходимо рассмотреть схему расположения помещений ресторана. (Рисунок 1.3) На рисунке представлено схематичное расположение помещений и указаны критические зоны ресторана.

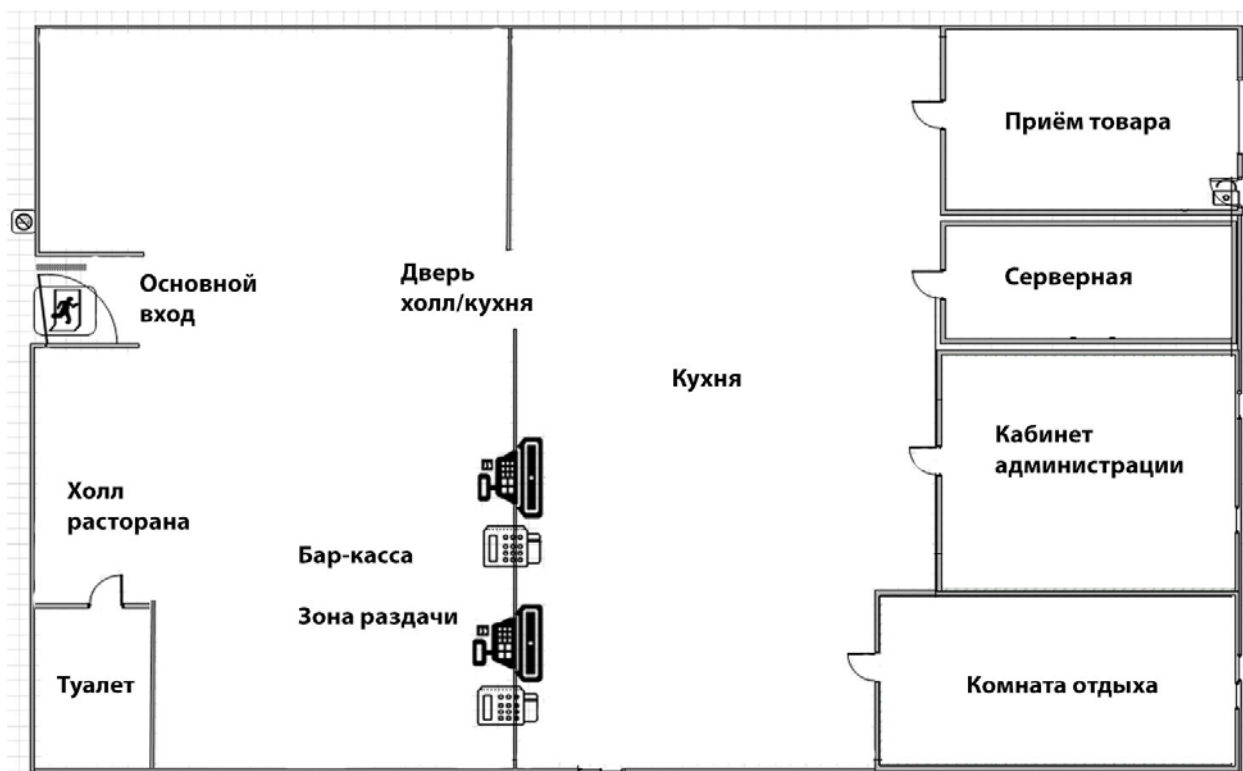


Рисунок 1.3. Схема помещений и критических зон ресторана.

Необходимо указать то, что ресторан находится на первом этаже торгового комплекса. Имеет собственные Основной вход и вход для приема товара. Ресторан имеет Холл для свободного посещения клиентами и служебная зона с помещениями, в которых могут находиться только сотрудники ресторана. Торговый комплекс имеет круглосуточную охрану, периметр комплекса имеет автономное видеонаблюдение, все входы и выходы, а также окна замкнуты в общую систему звуковой сигнализации несанкционированного доступа. Сигнализация активируется при закрытии торгового комплекса охраной, и деактивируется в начале дня.

После того, как выполнено описание объекта, можно переходить к построению матрицы безопасности. В таблице 1, представлена матрица безопасности ресторана «Макдоналдс».

Таблица 1. Матрица безопасности ресторана «Макдоналдс»

Номер	Название помещения	Функциональное назначение	Необходимые технические средства защиты
1	основной вход	свободный вход для посетителей ресторана в рабочее время	средства наблюдения, механический замок
2	бар-касса, зона раздачи	зона приема и выдачи заказов, оплата заказа	средства наблюдения, кнопка вызова охраны
3	прием товара	вход только для сотрудников ресторана	средства наблюдения, электромагнитный замок
4	комната отдыха	хранение вещей сотрудников и др.	средства наблюдения, кодовый замок
5	кабинет администрации	размещение управляющего, хранение наличных после съема кассы	средства наблюдения, электромагнитный замок, сейф, кнопка вызова охраны
6	серверная	размещение серверного оборудования	противопожарная дверь, серверный шкаф, кондиционер, кодовый замок
7	кухня	помещение для приготовления блюд	средства наблюдения
8	дверь холл/кухня	перемещение сотрудников ресторана между служебными помещениями и холлом ресторана	кодовый замок
9	холл ресторана	свободный доступ посетителей ресторана в рабочее время	средства наблюдения

Отдельное внимание необходимо уделить противопожарной безопасности.

Пожарная безопасность в ресторане состоит из таких элементов, как пожарная сигнализация, средства локализации и погашения пожара (огнетушители, средства огневой изоляции), схема эвакуации и направляющие к выходу указатели (световые таблички), система речевого громкого оповещения, умение персонала пользоваться противопожарными

системами и средствами. Необходимо вести контроль вентиляционной системы, системы автоматического удаления дыма. Ежемесячно проходить техническое обслуживание, от датчиков до вентиляции. Проводить чистку вентиляции по графику.

Так как исследуемый ресторан быстрого питания входит в состав торгового комплекса, то и система пожарной безопасности ресторана включена в общую систему противопожарной безопасности торгового комплекса. Во всех помещениях ресторана размещены схемы эвакуации, указатели выходов, система речевого громкого оповещения, датчики обнаружения дыма, кнопки пожарной сигнализации для ручного включения.

1.7. Описание информационной среды ресторана «Макдоналдс»

Кроме средств физической защиты и противопожарной безопасности, необходимо рассмотреть вопрос организации системы защиты цифровой информации.

В общем виде цель защиты информации определяется как обеспечение безопасности информации.

Основной целью защиты информации является обеспечение заданного уровня ее безопасности. Под заданным уровнем безопасности информации понимается такое состояние защищенности информации от угроз, при которых обеспечивается допустимый риск ее уничтожения, изменения и хищения. При этом под уничтожением информации понимается не только ее физическое уничтожение, но и стойкое блокирование санкционированного доступа к ней. В общем случае при блокировке информации в результате неисправности замка или утери ключа сейфа, забытия пароля компьютера, искажения кода загрузочного сектора винчестера и других факторах информация не искажается и не похищается и при определенных усилиях доступ к ней может быть восстановлен. Следовательно, блокирование информации прямой угрозы ее безопасности не создает. Однако при невозможности доступа к ней в нужный момент ее пользователь теряет информацию так же, как если бы она была уничтожена.

Под угрозой безопасности информации в компьютерной сети (КС) понимают событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

На рисунке 1.4 представлена схема расположения информационно-коммуникационного оборудования ресторана «Макдоналдс».

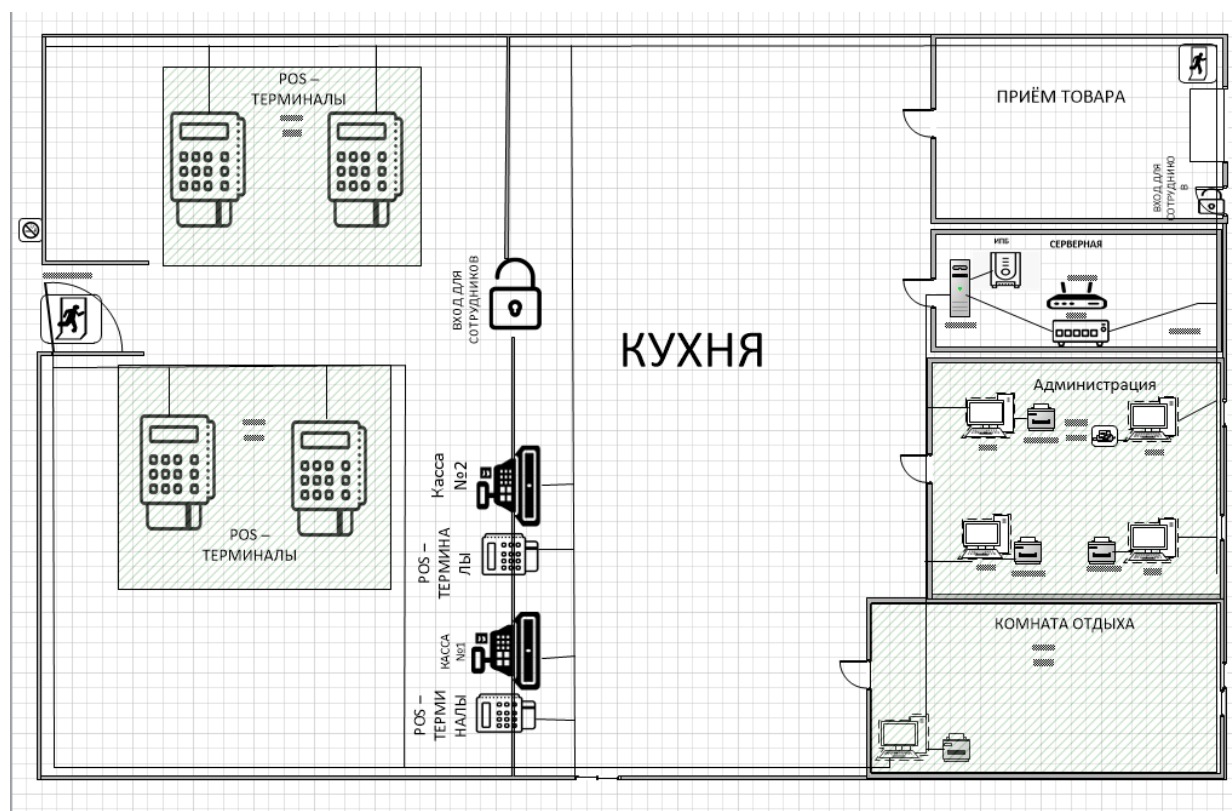


Рисунок 1.4. Схема расположения информационно-коммуникационного оборудования ресторана

Находящееся в ресторане информационно-коммуникационное оборудование и его функциональное назначение представлено в таблице 2.

Таблица 2. Информационно-коммуникационное оборудование ресторана

Место расположения	Название оборудования	Функциональное назначение
Холл	терминалы самообслуживания для клиентов ресторана (4 шт)	прием заказов; безналичная оплата; печать чека
Бар-касса	Касса 1 Касса 2 POS-терминал 1 POS-терминал 2	прием заказов; оплата наличными и безналичным способом; печать чека

Таблица 2. Продолжение

Кабинет администрации	Компьютеры администрации (4 шт); Локальные принтеры (4 шт)	составление, отправка отчетов, заказов; выход в Internet; подключение к удаленному серверу
Серверная	Сервер, Монитор Видеорегистратор Роутер Источник бесперебойного питания (ИБП)	подключение видеокамер наблюдения; настройка и управление видеонаблюдением; Internet-соединение; временное электропитание
Комната отдыха	Компьютер для сотрудников Локальный принтер	выход и internet; подготовка отчетов и документов сотрудниками; печать отчетных документов

Так как ресторан «Макдоналдс» располагается на территории торгового комплекса, то вертикальная часть LAN непосредственно ресторана, как таковая практически отсутствует. Провайдер Internet подвел оптоволоконный кабель ко всему торговому центру, а внутренние организации уже подключаются витой парой к коммуникационному оборудованию. Локальная сеть ресторана «Макдоналдс» в горизонтальной части организована по средствам беспроводной технологии WI-FI. Это позволяет отказаться от использования проводной коммуникации между оборудованием ресторана. Организация «гостевой» wi-fi подсети для подключения посетителей ресторана к Internet, не предусмотрена.

Таким образом, при рассмотрении вопросов первой главы выпускной квалификационной работы были подробным образом рассмотрены организационная структура ресторана «Макдоналдс», государственные нормативные документы, необходимые для организации работы ресторана «Макдоналдс», осуществлен анализ рисков и угроз для ресторана, построена матрица безопасности, выполнено описание информационной среды исследуемого ресторана «Макдоналдс».

ГЛАВА 2. РЕАЛИЗАЦИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ

2.1. Выбор средств физической защиты

Исходя из рисков и угроз для ресторана быстрого питания, необходимо сделать правильный выбор технических средств и оборудования для физической защиты.

Прежде чем приступить к выбору конкретных средств физической защиты, необходимо составить полный список требуемого оборудования:

- механический замок;
- электромагнитный замок;
- средства видеонаблюдения;
- кнопка вызова охраны;
- противопожарная дверь;
- сейф;
- серверный шкаф;
- кондиционер.

Чтобы предотвратить вход посторонних лиц в нерабочее время со стороны основного входа, необходимо и достаточно входную дверь оборудовать механическим замком. После снятия с охранной сигнализации торгового комплекса, администратор ресторана или лицо его заменяющее открывают основной вход для посетителей. Ключ от этого замка не выносится за пределы ресторана, и хранится в кабинете администрации ресторана. Он же осуществляет закрытие ресторана в конце рабочего дня.

Рынок механических замков очень широк. И выбрать достойный вариант не всегда бывает просто. Производителей подобных замков довольно много. Это дешёвые, но достойно зарекомендовавшие себя бюджетные серии для входных дверей турецких производителей. Например, Elementis, от бренда KALE KILIT или VORNE. Среднебюджетные серии замков для дверей от производителей WinkHaus и Maco. Безупречные лидеры на рынке дверной фурнитуры: ROTO FRANK и SIEGENIA AUBI, Apeks.

Осуществив анализ и проведя мониторинг достоинств и недостатков моделей различных производителей, принято решение о приобретении и установке замка фирмы Арекс. Представлен на рисунке 2.1.

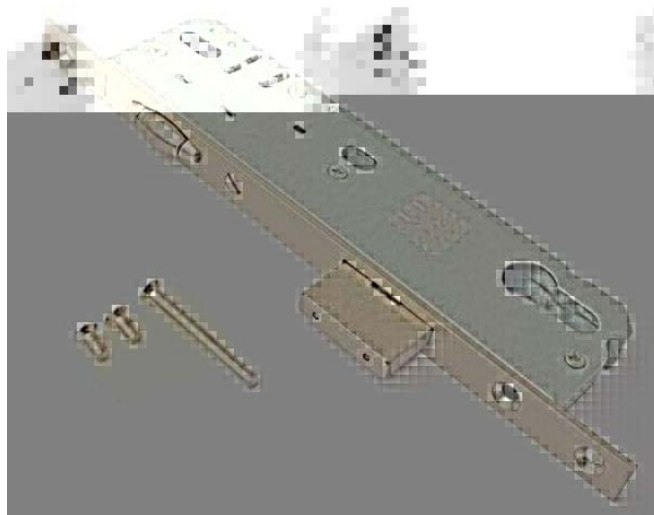


Рисунок 2.1. Замок врезной противопожарный Арекс 2000-Panic-ZN 0

Замок врезной цилиндрический Арекс 2000-Panic-ZN 0 (Апекс) с верхней роликовой защелкой. Рекомендован для установки в двери из алюминиевого профиля. Классический прямоугольный ригель с ходом 16 мм. Удаление ключевого отверстия 35 мм. В замок Арекс 2000-Panic-ZN 0 может быть установлен цилиндр евростандарта. Данный замок обеспечивает надежное запираение помещения. Предназначен для установки в двери из пластикового или алюминиевого профиля. Рекомендован для установки во входные двери. Роликовая защелка и отсутствие системы автоматического запирания, позволяют одновременно обеспечить и закрытое состояние двери (она не распахнута), и свободный выход посетителей ресторана, как в штатном, так и в экстренном режиме, например в случае эвакуации при пожаре. Технические характеристики изделия представлены в таблице 3.

Таблица 3.

Назначение	Двери из алюминиевого профиля
Рекомендован для установки в входные двери	Да
Рекомендован для установки в межкомнатные двери	Да
Тип крепления врезн. замка	Лицевая планка
Тип ригелей	Классический/Прямоугольный
Вылет ригелей	16 мм
Удаление ключевого отверстия (Backset)	35 мм
Тип механизма секретности	Цилиндровый
Тип цилиндрического механизма	Евроцилиндр
Защелка	Роликовая
Автоматическое запирание	Не автоматическое
Количество точек запирания	1

Следующим техническим средством предотвращения доступа посторонних лиц в помещения ресторана как в рабочее, так и в нерабочее время, является электромагнитный замок. Подобным типом замка необходимо оборудовать следующие критические зоны ресторана. Это Вход приема товара, Кабинет администрации, Серверная, Дверь холл/кухня, Комната отдыха. Всего 5 зон.

На самом деле электронные замки стали появляться на прилавках магазинов достаточно давно. Изначально они открывались исключительно после ввода PIN-кода, но сейчас существуют и гораздо более интересные модели. Чаще всего их отличают по методу открытия: Электронный замок с NFC или RDIF-картой — открывается при помощи смартфона, в котором имеется соответствующий чип. Впрочем, вместе с замком могут поставляться NFC-метки, похожие на ключ для домофона — для открытия замка можно использовать и их. Электронный биометрический замок — располагает сканером отпечатка пальца. В его памяти могут содержаться узоры на пальцах сразу нескольких людей, что позволяет пользоваться замком многочисленным сотрудникам находящегося за дверью помещения. Подобные замки начали выпускать и известные уху компании — например,

несколько моделей произведены силами Samsung. Также замки отличаются по методу монтажа. Не особо дорогостоящие модели могут принадлежать к накладному типу. Такой замок можно выломать, особенно если перед злоумышленниками поставлена задача проникнуть в помещение любой ценой. Врезной умный замок гораздо надежнее, но и в монтаже он сложнее.

Многие умные электронные дверные замки располагают цифровой клавиатурой, т.е. являются кодовыми. Это значит, что открывать их можно и обычным методом — набрав соответствующий код. Некоторые модели способны похвастать и микрофоном, что позволяет поговорить с человеком, находящимся в помещении. Словом, умный замок — это по факту улучшение традиционного домофона, которым пользуются многие.

Проанализировав рынок, было принято решение о приобретении и использовании электромагнитного замка "Power Lock-280 Sklad". Представлен на рисунке 2.2.



Рисунок 2.2. Электромагнитный замок "Power Lock-280 Sklad"

"Power Lock-280 Sklad" это полностью собранный комплект для установки. Не нужно искать оборудование по отдельности.

Данный комплект может быть установлен на уличную дверь, считыватель со встроенным контроллером не подвержен воздействию влаги, мороза и перепадов температур.

Комплект подходит для дверей любого типа (из пластика, дерева или металла).

В комплект входят ключи-брелоки, с помощью которых можно открыть дверь, поднеся их к бесконтактному считывателю, а также мастер-карта для записи ключей в память устройства. В систему можно прописать большое количество дополнительных брелоков (до 2000). Также возможен ввод цифрового пароля от 4 до 8 символов.

Замок оснащен кнопкой выхода. Легкого касания кнопки выхода достаточно для разблокировки двери. Такое исполнение прослужит достаточно продолжительное время. Изделие снабжается доводчиком двери в комплекте для плавного закрытия двери и корректной работы электромагнитного замка. Основные технические характеристики представлены в таблице 4.

Таблица 4. Основные технические характеристики электромагнитного замка "Power Lock-280 Sklad"

Электромагнитный замок: Усилие на отрыв: 280 кг Напряжение питания: 12 В Вес: 1,1 кг Размер замка: 190x32x22 мм
Доводчик: Максимальный вес двери: 100 кг Максимальная ширина двери: 1200 мм Максимальный угол открытия: 180 градусов
Блок питания: Входящее напряжение: 220В; Выходящее напряжение: 12В; Рабочая температура: от – 10 до +50 мм.
Считыватель со встроенным контроллером: Поддержка карт и брелоков: EM-Marine Дистанция считывания: 2 см Температура работы: от -40 до +60 градусов Допустимая влажность: 20%RH - 90RH% Емкость памяти: 2000 карт Материал: металл+пластик
Кнопка выхода: Контакты: NC, NO, COM Материал: пластик

Самым полезным техническим средством обеспечения безопасности ресторана является видеоконтроль с сохранением записей. Эта система позволяет вести круглосуточную съемку всех помещений и критических зон ресторана. При необходимости всегда возможно организовать просмотр того или иного события, восстановив его из сохраненных записей. Согласно части 2 статьи 26.7 КоАП РФ, видеозапись служит доказательством в случае разбирательства административного правонарушения (мелкое хулиганство, порча имущества). Сохраненные файлы могут помочь установить процесс совершенного преступления (УПК РФ, статьи 81 и 84) либо выявить нарушения служебных обязанностей (АПК РФ, статья 64, пункт 2).

Видеонаблюдение дисциплинирует и гостей, и сотрудников ресторана. Первые, таким образом, защищаются от конфликтных ситуаций, краж, порчи имущества ресторана, других противоправных действий. Вторые: обеспечивается трудовая дисциплина, пресекаются конфликты, противоправные действия, махинации с кассой, контролируется соблюдение правил техники трудовой и пожарной безопасности, соблюдение рецептов приготовления блюд.

Необходимо обеспечить законность видеосъемки. Посетители оповещаются установкой таблички с уведомлением о проведении записи (русский язык – обязательное требование). Информационный знак переносит ответственность на посетителя: клиент сам определяет, посещать такое заведение либо нет.

Также необходимо заручиться письменным согласием всего персонала.

В Правила внутреннего трудового распорядка вносятся пункты о мониторинге трудовой деятельности. Необходимо указать обоснование нововведений: безопасность сотрудников и посетителей, контроль качества обслуживания, предупреждение противоправных деяний.

Дополнительно создается Положение о видеонаблюдении, регламентирующее количество и местоположение камер, а также уровень

доступа персонала. Просматривать записи могут только лица, уполномоченные выносить взыскания и штрафы. Оборудование нельзя монтировать в туалетах, врачебных кабинетах, раздевалках и комнатах отдыха.

Указанные изменения необходимо утвердить в приказе. В документе указывают дату начала ведения записей и перечень ответственных за работу видеонаблюдения лиц. Должности сотрудников, имеющих доступ к данным камер, также вносятся в Положение о защите персональных данных.

Зафиксировать правила необходимо и в трудовом договоре сотрудников, для этого в раздел «Условия труда» добавляют следующую фразу: «Работник осведомлен и согласен с использованием работодателем системы видеонаблюдения в целях обеспечения безопасности работника и работодателя».

Для реализации проекта удобнее всего воспользоваться готовой системой наблюдения, в которую входят:

- влаго- и пылезащищенные всепогодные камеры в антивандальном исполнении;
- видеорегистратор или рекордер (записывающее устройство) с несколькими каналами подключения;
- жесткий диск для хранения информации;
- кабели для соединения камер с рекордером;
- блоки питания, необходимые аксессуары и инструкции.

Дополнительно потребуется обычный компьютерный монитор или телевизор. Видео с камер, выводится на экран в режиме реального времени. Одновременно идет запись происходящих событий. Информация, распределенная по датам и номерам видеокамер, хранится на жестком диске. Архив можно просмотреть в любой момент времени.

Прежде чем приступать к выбору системы, необходимо определиться с количеством камер видеонаблюдения и их месторасположением. Схема размещения камер видеонаблюдения представлена на рисунке 2.3.

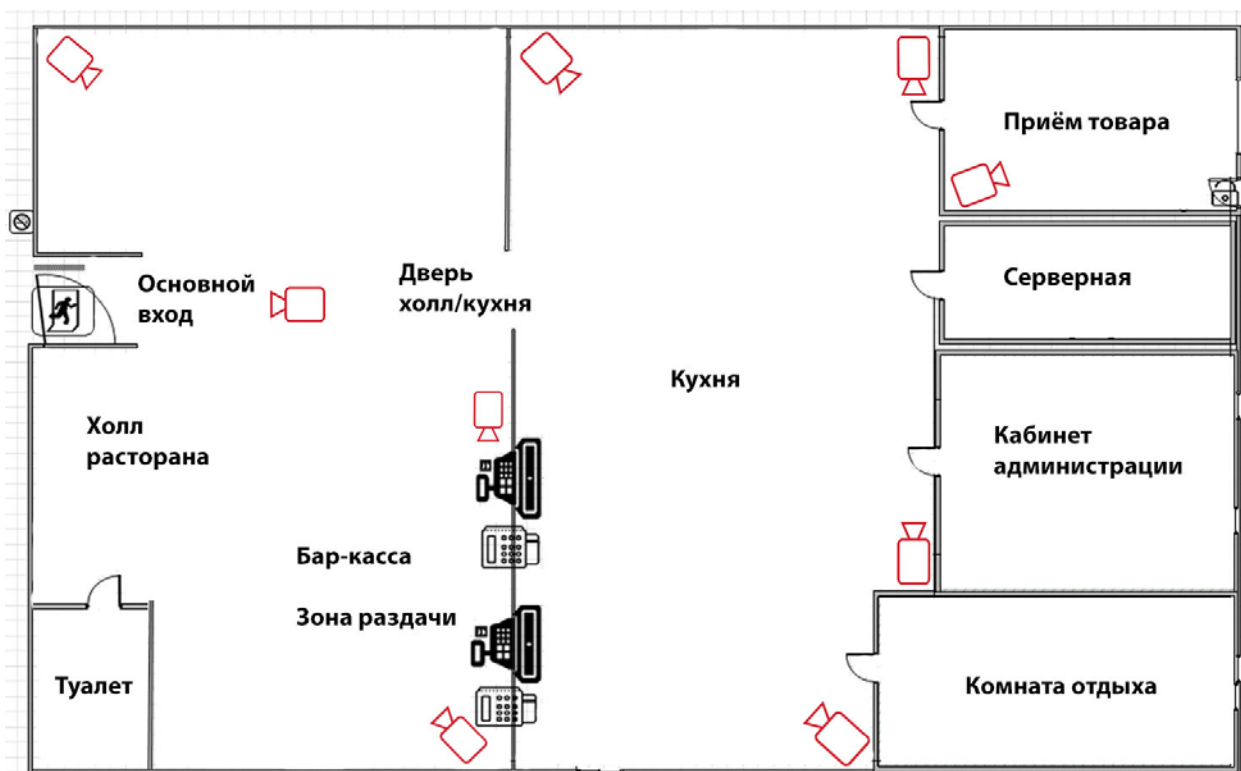


Рисунок 2.3. Схема расположения камер видеонаблюдения в ресторане

Всего требуется как минимум 9 камер. Они в достаточной мере обеспечивают видеоконтроль всех критических зон ресторана быстрого питания.

После анализа рынка, принято решение о приобретении системы видеонаблюдения AND 5Мп Ps-Link KIT-A216HD 16 камер для помещения. Комплект AND видеонаблюдения состоящий из видео регистратора и 16-ти купольных FullHD камер (1080P). Решение на основе AND позволяет в режиме онлайн контролировать помещения без задержек и потери качества видеоизображения. При необходимости возможно заменить некоторое количество камер уличными для контроля за территорией. Комплект содержит все необходимые комплектующие для монтажа. Для хранения записей видеонаблюдения возможно установлен жесткий диск емкостью 4Тб. Комплект представлен на рисунке 2.4.



Рисунок 2.4. Комплект видеонаблюдения AHD 5Мп Ps-Link KIT-A216HD 16 камер для помещения

Схема подключения комплекта видеонаблюдения представлена на рисунке 2.5.

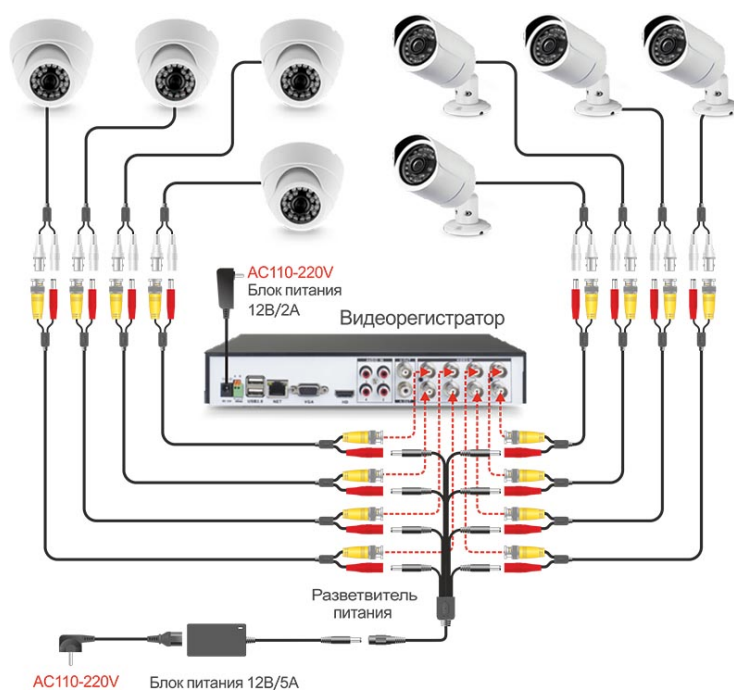


Рисунок 2.5. Схема подключения комплекта видеонаблюдения AHD 5Мп Ps-Link KIT-A216HD

Данная система обладает следующими преимуществами:

- Системы видеонаблюдения PS-Link собираются в России;
- Широкий угол обзора камер 85°;
- Высокое качество изображения FullHD;
- Температурный диапазон работы камер от -20 до +50;

- При подключении комплекта к сети Интернет, возможно следить за объектом из любой точки мира при помощи своего телефона, ноутбука, компьютера;
- Объем жесткого диска на 4Тб позволяет хранить видеоархив до 2-х недель в максимальном качестве изображения;
- Видеокамеры данных комплектов имеют встроенную инфракрасную подсветку на 30 метров с автоматическим переключением день/ночь.

Технические характеристики оборудования представлены в таблице 5.

Таблица 5.

Видео • Формат записи: D1 (704x576)/ 960H (928x576)/ 720P (1280x720)/ 1080N (960x1080) • Частота кадров: D1 22fps/ 960H 22fps/ 720P 22 fps/ 1080N 12fps • Видео вход: 16 BNC • Видео выход: 1 канал BNC, 1 канал VGA, 1 канал выход HDMI
Аудио • Аудио вход: 1 канал RCA • Аудио выход: 1 канал
Запись и проигрывание • Режим записи: Ручной режим, по детектору движения, по расписанию • Проигрывание: Воспроизведение 4-х каналов • Хранение записей: Жесткий диск формата 3.5" SATA • Режим резервного копирования: Сеть, USB накопитель
Дополнительные порты • Сетевой порт: RJ45 10Mб / 100Mб • Порт USB: 2 x USB 2.0 • Порт HDD: 1 x HDD SATA 4000 Гб формат 3.5"
Другое • Электропитание: Внешний источник питания DC 12V / 2A • Рабочая температура: -10°C....+55°C • Рабочая влажность: 10%-90%
Видеокамера купольная (для помещений) • Матрица: 5Мр • Разрешение: 1920x1080px • ИК-подсветка: 24 IR LED светодиода • Дальность ИК-подсветки: До 30 метров • Светочувствительность: 0Лк при вкл. ИК подсветке



Рисунок 2.6. Пример ручного режима настройки камер

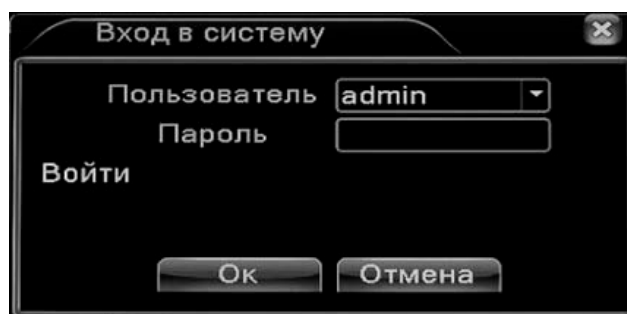


Рисунок 2.7. Окно входа в систему

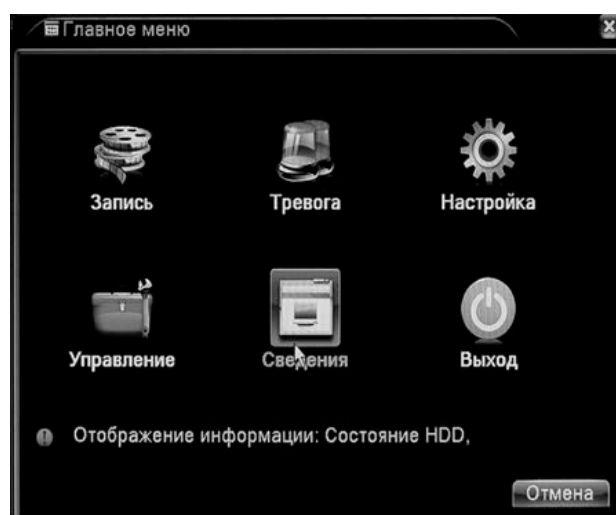


Рисунок 2.8. Окно Главного меню

Следующим техническим устройством системы комплексной защиты ресторана быстрого питания, является кнопка вызова охраны. На территории торгового центра для решения этой задачи применяется радиоканальная

охранная система РИФ РИНГ-701.

Назначение системы РИФ РИНГ-701 заключается в следующем:

- организация индивидуальной охраны людей;
- охрана стационарных объектов с передачей тревожных извещений по радиоканалу на стационарные и носимые приёмники;
- радиоканальное удлинение шлейфов сигнализации проводных охранно-пожарных систем;
- создание вызывных систем различного назначения.

Таким образом, административные сотрудники ресторана в рабочее время обязаны при себе иметь беспроводную тревожную радиокнопку Риф Ринг RR-701TM. Представлена на рисунке 2.9.



Рисунок 2.9. Беспроводная тревожная радиокнопка Риф Ринг RR-701TM

Тревожная радиокнопка Риф Ринг RR-701TM представляет собой миниатюрный носимый радиопередатчик, предназначенный для беспроводной передачи извещений о нападении на граждан, на охраняемые объекты и т.п. Дальность передачи тревожных радиосигналов в условиях прямой видимости составляет около 400 м. Сертификат соответствия No РОСС.RU.ME30.B00722.

В функции тревожной кнопки входит трансляция данных о несанкционированном проникновении на объект. Такая тревожная кнопка может быть использована и для вызова экстренной медицинской помощи

либо для оповещения о чрезвычайных ситуациях.

Кроме этого, в зоне Бар-касса необходимо установить стационарную радиокнопку RR-701TK3. Представлена на рисунке 2.10.



Рисунок 2.10. Радиокнопка для стационарной установки RR-701TK3

Это радиокнопка большого радиуса действия для стационарной или скрытой установки с автономным питанием.

Такая радиосистема позволяет сотрудникам ресторана быстрого питания в любое время незамедлительно вызвать охрану торгового комплекса.

Следующее техническое устройство, необходимое для комплексной защиты ресторана быстрого питания – это сейф в кабинете управляющего.

Какое бы назначение, вид, тип не имел сейф, его главная функция – защита от несанкционированного проникновения и сохранение в целостности содержимого. То есть он должен выдержать взлом, пожар, удары, воду, взрыв и другое неблагоприятное воздействие. Степень надежности определяется системой стандартизации, которая в разных странах различная. В России она соответствует европейским стандартам и подразумевает наличие 11 классов взломостойкости, которые проверяются в лабораторных условиях профессиональными экспертами.

В ресторане сейф необходим для:

- хранения отчетной документации в бумажном виде;

- временное хранение наличных денежных средств до процедуры инкассации;
- хранение ключа от замка основного входа в ресторан;
- хранение запасных брелоков, ключ-карт и программатора от электромагнитного замка;
- хранение документации с логинами и паролями от оборудования.

Рынок сейфов широк и разнообразен. Осуществив анализ предложений, принято решение о приобретении огневзломостойкого сейфа Гранит 90Т EL. Представлен на рисунке 2.11.



Рисунок 2.11. Сейф огневзломостойкий Valberg Гранит 90Т EL

Сейф огневзломостойкий Гранит 90Т EL устойчивость к взлому по ГОСТ Р 50862-2012: класс 1 (РСБ-С); класс 2 (ГОСТ Р). Обладает огнестойкостью по ГОСТ Р 50862-2012: класс 30Б (РСБ-С), класс 30Б (ГОСТ Р). При заливке двери и корпуса сейфа используется специальный тяжелый бетон, корпус сейфа и дверь заливные; толщина стенок - 40 мм. Сейф снабжен 3-х сторонней усиленной ригельной системой запирания, предусмотрена защита замка и ригелей от высверливания и выбивания, а также система блокировки ригельного механизма при выбивании замка. Сейф комплектуется кодовым электронным замком PS 600 (ПРОМЕТ, класс В, ГОСТ, ECB-S). Характеристики сейфа гарантируют надежную сохранность всего содержимого в любой критической ситуации. Тот факт,

что сейф оборудован возможностью анкерного крепления к полу при весе 205 кг, практически исключает возможность злоумышленнику вынести сейф из помещения ресторана.

Следующим компонентом комплексной системы защиты ресторана быстрого питания является противопожарная дверь в помещение серверной. Согласно СП 5.13130.2009 предел огнестойкости серверной должен быть следующим: перегородки - не менее EI 45, стены и перекрытия - не менее REI 45. Т.е. в условиях пожара помещение должно оставаться герметичным в течение 45 минут, препятствуя дальнейшему распространению огня.

Помещение серверной должно быть отдельным помещением, функционально не совмещенным с другими помещениями. К примеру, не допускается в помещении серверной организовывать мини-склад ИТ-оборудования или канцелярских товаров.

Дверь в помещение серверной также должна обеспечивать требования по огнестойкости (не менее EI 45). Необходимо использовать противопожарную дверь.

Противопожарные двери – это двери, специальная конструкция которых препятствует распространению пожара из центра возгорания в прилегающие помещения в течение определенного времени.

Существуют установленные функциональные требования к противопожарным дверям:

- удерживать огонь до приезда пожарных бригад;
- дать возможность людям выбраться из помещения при пожаре;
- помешать дыму проникнуть внутрь помещения, чтобы люди не отравились углекислым газом;
- выдержать длительное воздействие огня и не дать огню распространиться дальше по зданию.

Дым в помещение не пропускают терморасширяющиеся ленты - резиновые уплотнители по периметру полотна. При воздействии жара уплотнители расширяются, повышая герметичность двери. Известно, что

большая часть жертв пожара погибают от отравления угарным газом. Противопожарная дверь снижает эти риски.

Удержание огня зависит от материалов, которыми заполнено полотно двери. Минеральная вата или поролон не справятся с этой задачей. Материалы должны быть самозатухающими, то есть не поддерживать горение без воздействия огня - например, базальтоволоконная плита из каменных пород.

Исходя из требований противопожарной безопасности, был осуществлен мониторинг и анализ рынка дверей, требуемого типа. По результатам принято решение о приобретении следующей модели: дверь противопожарная ДПО-1 Bravo остекленная, представлена на рисунке 2.12.



Рисунок 2.12. Дверь противопожарная ДПО-1 Bravo остекленная

При изготовлении двери используется высокопрочное полотно типа "сэндвич" из оцинкованной холоднокатанной стали с заполнением из минераловатной плиты высокой плотности. Наличие огнестойкого стекла, позволяет в случае пожара убедиться, не остался ли кто-то в закрытом

помещении. Характеристики противопожарной двери ДПО-1 представлены в таблице 6.

Таблица 6. Характеристики противопожарной двери ДПО-1

Тип:	остекленные
Стекло:	Противопожарное стекло 300*400*22 мм (триплекс), с рамкой на винтах - 2 шт
Усиление:	Дополнительную защиту обеспечивают противосъемные штыри (2 шт)
Крепление:	Двери крепятся анкерными болтами через коробку
Открывание:	180°
Уплотнитель:	Два контура износостойкого уплотнителя (ТЭП-термоэластопласт)
Утепление полотна:	Негорючая минераловатная плита высокой плотности (130кг/м ²). Высокий показатель тепло- и звукоизоляции, влаго- и воздухопроницаемости.
Толщина стали, мм:	1
Страна:	Россия

Следующим физическим элементом в системе комплексной защиты ресторана быстрого питания является серверный шкаф. Назначение серверного шкафа заключается в следующем:

- компактное расположение телекоммуникационного, серверного, электротехнического и распределительного оборудования;
- обеспечение удобного доступа к обслуживанию устройств, размещенных в шкафу;
- соблюдение оптимального температурного режима при эксплуатации оборудования, кондиционирование, охлаждение систем;
- защита высокотехнологичных устройств от несанкционированного доступа, загрязнения, запыления элементов.

Серверные шкафы различают по типу конструкции:

- настенные, у которых ограничена глубина (не более 600 мм), в них размещают роутеры, хабы, свитчи;
- напольные, способные выдерживать тяжелые устройства,

используются под серверы, источники бесперебойного питания.

Осуществив анализ различных производителей и типов серверных шкафов, для реализации задач данной дипломной работы, был выбран напольный шкаф ЦМО ШТК-М-18.6.6-4ААА, представлен на рисунке 2.13.



Рисунок 2.13. Напольный серверный шкаф ЦМО ШТК-М-18.6.6-4ААА

Общие характеристики серверного шкафа представлены в таблице 7.

Таблица 7. Характеристики серверного шкафа

Тип	шкаф
Монтажная ширина стойки (rack)	19"
Высота в юнитах	18 U
Монтаж	напольный
Комплектация	передняя дверь, боковые панели
Класс защиты	IP20
Особенности	перфорированная дверь
Ширина	600 мм
Высота	960 мм
Глубина	600 мм

Так как оборудования в серверной ресторана быстрого питания не так много, представленный шкаф легко разместит в себе всё необходимое.

Перфорированная дверь способствует лучшему охлаждению установленным в шкаф компонентам.

Для защиты от перегрева установленного в серверный шкаф оборудования, необходимо снабдить серверную комнату системой поддержания заданного микроклимата.

К серверным комнатам предъявляются особые требования:

- Температура воздуха не должна превышать 25 градусов. Оптимальным уровнем является диапазон между 15 и 22 градусами выше нуля;

- Влажность: летом – не выше 65%, зимой 75%;
- Скорость воздушных потоков не должна превышать 0,3 м/с и не должна быть ниже 0,5 м/с;

- Уровень пыли должен быть минимальным;

- Уровень шума не выше 65 дБ.

Чтобы избежать возможных негативных последствий, в серверных помещениях устанавливаются кондиционеры. Они эффективно решают следующие задачи:

- Поддерживают оптимальный температурный режим;
- Способствуют очищению воздуха от пыли;
- Контролируют влажностный режим.

Осуществив мониторинг и анализ различных предложений, была выбрана настенная сплит-система LG P09SP2. Представлена на рисунке 2.14.



Рисунок 2.14. Настенная сплит-система LG P09SP2

LG P09SP2 — настенный кондиционер инверторного типа. На компрессор действует гарантия производителя 10 лет. Низкий уровень шума 19 дБ, что является одним из самых низких показателей в мире. Фильтр двойной защиты DUAL задерживает частицы пыли крупнее 10 мкм. Данная модель кондиционера прекрасно справится с возложенными задачами.

Все технические характеристики указанной модели представлены в таблице 8.

Таблица 8. Технические характеристики сплит-системы LG P09SP2

Площадь помещения:	25 кв.м
Компрессор:	Инвертор
Мощность охлаждения:	2,5 кВт
Мощность обогрева:	2,5 кВт
Параметры питающей сети:	220 - 240 / 50
Потребляемая мощность охлаждения:	0,63 кВт
Потребляемая мощность обогрева:	0,69 кВт
Уровень шума внутреннего блока:	22/42
Максимальная длина трассы:	15 м
Перепад высот:	7 м
Размер внешнего блока (ШхВхГ):	717×483×230 мм
Размер внутреннего блока (ШхВхГ):	837×308×192 мм
Вес внешнего блока:	25.5 кг
Вес внутреннего блока:	9.7 кг

Итак, в данном разделе было рассмотрено и обоснован выбор всех технических средств для создания комплексной системы защиты ресторана быстрого питания.

2.2. Выбор информационно-коммуникационного оборудования

Осуществив выбор технических средств для создания комплексной системы защиты ресторана быстрого питания, необходимо определиться с информационно-коммуникационным оборудованием.

Часть оборудования данного типа уже описывалась ранее, при выборе системы видеонаблюдения — это видеорегистратор и видеокамеры наблюдения. Далее необходимо выбрать:

- терминал самообслуживания 1, 2, 3, 4;

- кассовый аппарат;
- pos-терминал оплаты;
- компьютеры администрации;
- роутер;
- монитор;
- источник бесперебойного питания (ИБП).

Новые технологии в автоматизации ресторанов меняют привычные методы обслуживания гостей. Компактные мобильные терминалы официантов, планшеты для самостоятельного заказа и киоски самообслуживания набирают все большую популярность. Они широко используются в крупных фастфуд-сетях.

Терминалы (киоски) имеют большой успех среди посетителей, потому что дают полный контроль над заказом и позволяют избежать недопониманий. Технология удобна не только для гостей — это настоящая находка и для рестораторов.

В популярных фастфуд-заведениях часто бывают длинные очереди на кассу, особенно в часы пик. Благодаря киоскам самообслуживания можно разгрузить поток гостей, тем самым сократив время на прием заказа. А благодаря интеграции с POS-системой заказ моментально попадет на кухню и будет готовиться в порядке общей очереди. В итоге установка киосков помогает обслуживать больше посетителей и принимать больше заказов.

Чтобы обслуживать большое количество людей без киосков, нужно расширять штат и нанимать новых сотрудников. А благодаря современной технологии можно снизить расходы на персонал. Главное, чтобы у киоска самообслуживания был интуитивно понятный и простой интерфейс. В обратном случае потребуется еще больше сотрудников, чтобы помогать гостям с заказом.

В отличие от заработной платы, которую нужно платить каждый месяц, киоски — дорогостоящее, но разовое вложение. А благодаря их

установке можно перераспределить рабочую силу в ресторане и использовать сотрудников на других позициях, где они смогут принести больше пользы.

Киоск самообслуживания — отличный инструмент для улучшения продаж. Во-первых, можно добавить красивые и аппетитные картинки блюд, которые далеко не всегда можно уместить в обычном меню. А картинки вместе с грамотным описанием — супер комбо, которое подталкивает к покупке. Во-вторых, можно настроить персональные рекомендации дополнительных блюд, напитков, соусов и так далее. В этом плане возможности киосков почти безграничны.

Выбор терминалов самообслуживания для ресторанов быстрого питания, довольно широк. Осуществив анализ рынка, принято решение о приобретении киоска самообслуживания для фастфуда «Q-50». Представлен на рисунке 2.15.

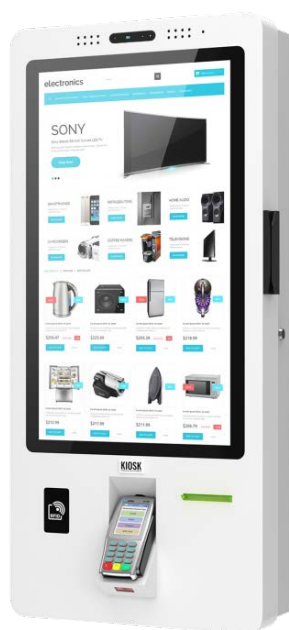


Рисунок 2.15. Киоск самообслуживания для фастфуда «Q-50»

Терминал самообслуживания «Q-50» выполнен в тонком эргономичном корпусе с возможностью монтажа на стену или стальную штангу, закрепленную между потолком и полом. Устройство оборудовано большим монитором (диагональ — 22-32 дюйма) с повышенной яркостью и контрастностью, сенсорным экраном multitouch (множественные касания), принтером с поддержкой онлайн-ККТ и POS-терминалом для приёма оплаты

картами.

Киоск рассчитан на установку в ресторанах быстрого питания (фастфуд). Основное назначение — автоматизация приёма заказов и оплаты за них. Торговая розница может использовать терминал «Q-50» для онлайн-продаж в магазинах, доступа к электронным каталогам и программам лояльности. Для таких приложений на киоск может быть установлено программное обеспечение eMenu Kiosk или R-Keeper. Параметры базовой комплектации указаны в таблице 9.

Таблица 9. Характеристики киоска самообслуживания для фастфуда «Q-50»

Стальной корпус настенного типа;
Рабочая температура — от 0 до 40 °С;
Сенсорный дисплей высокого разрешения (1920 x 1080) диагональю 32 дюйма с поддержкой multitouch;
Работа через защитное стекло;
Системный компьютер Intel Celeron (i3 или i5);
Память 2 или 4 Мб;
HD 500 Гб;
Устройство работы с картами Visa, Mastercard, PayPass, PayWave;
Поддержка бесконтактных мобильных платежей Android Pay и Apple Pay;
Чековый принтер с для печати на бумаге шириной 60-80 мм;
Совместимость с онлайн-кассами;
Устройство чтения одномерных и двумерных штрих-кодов;
Питание (энергосберегающее) — AC 110В/220В с ИБП, рассчитанным на автономную работу до 15 мин.;
Коммуникации — GPRS/3G, Ethernet, Wi-Fi;
ПО и ОС — Windows 10 IoT Enterprise, драйверы к компонентам

Далее необходимо определиться с кассовым аппаратом. Для ресторана быстрого питания следует выбрать современное решение – это онлайн-касса.

Онлайн-касса — это устройство, передающее фискальные данные в налоговую службу через интернет. В этом ее главное отличие от классической. Это нужно для прозрачности финансовых операций и облегчения работы службы — теперь инспектор видит все кассовые операции на экране своего монитора и может реже ходить на проверки. С

введением онлайн-касс должна уйти в прошлое двойная и тройная бухгалтерия, серые схемы и прочие атрибуты нелегального рынка.

Продвинутые онлайн-кассы очень удобны чисто функционально — они сами считают сумму покупки, к ним можно подключить любое вспомогательное оборудование — весы, сканер штрих-кода, банковский терминал. Общая схема онлайн-кассы представлена на рисунке 2.16.



Рисунок 2.16. Общая схема онлайн-кассы

Выбор самого кассового аппарата зависит от формата заведения. Имеет значение наличие в ассортименте крепкого алкоголя и пива, количество посетителей и другие факторы.

Кассовый аппарат для кафе, бара или ресторана лучше выбрать с тачскрином, так как работники вводят заказ и управляют бронированием столов прямо с экрана кассы прикосновением пальца или любого предмета — карандаша, пластиковой карты или стилуса. Подходящим вариантом в этом случае будет сенсорный POS-терминал. Для печати чеков и их отправки в ОФД нужен фискальный регистратор с широкой лентой. Для фиксации продажи алкоголя — сканер, считывающий 2D-штрихкоды на акцизной продукции.

Для реализации задач данной дипломной работы выбран комплект с кассой для точек с большой проходимостью на основе POS-терминал АТОЛ

VIVA Smart. Представлена на рисунке 2.17.



Рисунок 2.17. Комплект POS-терминал АТОЛ VIVA Smart

В комплект входит:

- POS-терминал АТОЛ VIVA Smart удобен для работы карандашом или пластиковой картой, влагозащитный экран спокойно можно размещать на баре;
- Фискальный регистратор Viki Print 80 Plus Ф: скорость печати — 300 мм/сек, есть автоотрезчик;
- 2D-сканер штрихкодов Newland HR3280 Marlin II;
- Денежный ящик АТОЛ ЕС-410-В;
- Принтер чеков для кухни, чтобы повар оперативно получал заказ и сообщал о его готовности.

Все компоненты комплекта могут соединяться друг с другом как проводным соединением (Ethernet), так и беспроводными WI-FI или Bluetooth.

Онлайн-касса также удобно оснастить мобильным POS-терминалом. Для использования в ресторане быстрого питания выбран POS-терминал Ярус М2100Ф. Представлен на рисунке 2.18. POS-терминал в фискальном исполнении (онлайн-касса) для торговой розницы и сферы услуг. Устройство соответствует требованиям 54-ФЗ и внесено в госреестр ККТ. Мобильная касса работает со всеми видами платежных карт: Визу, Мастеркард, Мир.



Рисунок 2.18. POS-терминал Ярус М2100Ф

Технические параметры POS-терминала Ярус М2100Ф представлены в таблице 10.

Таблица 10. Технические параметры POS-терминала Ярус М2100Ф

Монохромный дисплей размером 160 x 80 или цветной LCD-дисплей 320 x 240;
Процессор и память: ARM9 180 MHz, 16 Мб Flash, внутренняя память CPU 64Кб, 16/32 Мб SDRAM, защищенная память 4 Кб;
Чековый принтер для печати на бумаге шириной 58 мм со скоростью 75 мм/сек при разрешении 384 точки);
3-полосный считыватель карт (ISO7816 Smart Cards EMV 4.3 Level 1,2);
Поддержка бесконтактных платежей: обмен данными по протоколу ISO 14443-3/4; Работа с любыми бесконтактными технологиями, включая PayWave, PayPass, Apple Pay, Samsung Pay, все чипы семейства Mifare;
Связь: современный Wi-Fi с увеличенным диапазоном частот / двухсимвольные модемы 2G/3G;
Современная Li-Polymer аккумуляторная батарея на 3000 мАч, которая не реагирует на изменение температур, мало весит и долго держит заряд.

Далее необходимо подобрать компьютеры для администрации ресторана. Для этого удобнее всего использовать ноутбуки. После анализа рынка, для приобретения был выбран ноутбук ASUS X545FA-BQ189T. Представлен на рисунке 2.19.

Ноутбуки фирмы ASUS обладают высокой надежностью и производительностью. Позволяют реализовать широкий спектр возложенных на них задач. Данная модель прекрасно справится с выполнением рабочих процессов в ресторане быстрого питания.



Рисунок 2.19. Ноутбук ASUS X545FA-BQ189T

Основные характеристики ноутбука ASUS X545FA-BQ189T представлены в таблице 11.

Таблица 11. Основные характеристики ноутбука ASUS X545FA

экран: 15.6" (1920x1080)
процессор: Intel Core i5 10210U (4x1600 МГц)
оперативная память: 8 ГБ DDR4 2400 МГц
накопители: HDD 1000 ГБ, SSD 256 ГБ
встроенная видеокарта: Intel UHD Graphics 620
разъемы: USB 2.0 Type A x 2, USB 3.1 Type A, выход HDMI, микрофон/наушники Combo
беспроводная связь: Wi-Fi 802.11ac, Bluetooth 4.1
емкость аккумулятора: 32 Вт·ч
операционная система: Windows 10

Каждый сотрудник администрации имеет свой ноутбук со своим личным паролем, который не разглашается и назначается системным администратором.

Для просмотра видеозаписей, а также настройки интернет соединения и роутера, необходимо наличие компьютерного монитора. После анализа рынка выбран монитор Samsung S24F350FHI 23.5". Представлен на рисунке 2.20.

Монитор обеспечивает аккуратное и стабильное воспроизведение цветов, широкие углы обзора и малое время отклика (4мс). Он обладает оригинальным дизайном и высококачественной ЖК-панелью, изготовленной по технологии PLS, оборудован входами подключения HDMI, VGA.



Рисунок 2.20. Монитор Samsung S24F350FHI 23.5"

Для гарантии бесперебойного питания сетевого оборудования и системы видеонаблюдения, необходимо использовать источник бесперебойного питания (ИБП). Осуществив поиск, был выбран ИБП APC Smart-UPS SMT1000RMI2U. Представлен на рисунке 2.21.



Рисунок 2.21. ИБП APC Smart-UPS SMT1000RMI2U

ИБП позволяет оборудованию продержаться на батарейной поддержке около 2 часов. Относится к типу line-interactive. Также возможен монтаж в 19" стойку (серверный шкаф).

Завершающим оборудованием является роутер. Он необходим для поддержания интернет соединения всех подключенных устройств. Роутер должен обеспечивать постоянное, стабильное Internet соединение и соединение wi-fi, быть мощным и отказоустойчивым.

Осуществив анализ рынка, сопоставив сильные и слабые стороны роутеров разных производителей, принято решение о приобретении модели роутера Keenetic Giga (KN-1010). Представлен на рисунке 2.22.



Рисунок 2.22. Интернет-центр Keenetic Giga (KN-1010)

Данная модель роутера является наиболее надежной и современной. Обладает максимальными параметрами по управлению доступом, по настройке соединений, скоростью соединений. Обладает функциями DHCP-сервера, межсетевого экрана (Firewall), VPN, возможность подключения 3G/4G-модема.

Выбор физических средств защиты и необходимого коммуникационного оборудования закончен.

2.3. Выбор средств защиты информационно-коммуникационного оборудования

После завершения выбора физических средств защиты и информационно-коммуникационного оборудования необходимо перейти к выбору средств защиты этого оборудования и его настройке.

Грамотная настройка информационно-коммуникационного оборудования позволит уже на этом этапе существенно понизить риск несанкционированного доступа в локальную сеть ресторана, а также кражи

данных или их изменение при передаче через сеть Internet. Важным этапом является настройка роутера.

Необходимо отметить, что все устройства подключаются к роутеру по беспроводному подключению wi-fi, а возможность подключения устройств ограничена фильтрацией по MAC-адресам. Также wi-fi сеть является скрытой, изменен пароль администратора, отключена возможность удаленного администрирования роутера.

На рисунке 2.23 представлена настройка домашней подсети ресторана, включен DHCP сервер для раздачи ip-адресов сетевым устройствам, задан пул возможных адресов.

Домашняя сеть	
MAC-адрес	28:28:5d:b1:e7:3a
IP-адрес	192.168.1.1
Маска подсети	255.255.255.0
Сервер DHCP	Включен
Пул адресов	192.168.1.101 - 192.168.1.199
Точка доступа Wi-Fi	Включена
Имя сети (SSID)	K-DEP-INT2

Рисунок 2.23. Настройка домашней сети ресторана

Далее на рисунках 2.24 – 2.25 представлен пример настройки VPN-сервера.

Сервер VPN (PPTP)

Сервер VPN позволяет получить доступ к устройствам вашей домашней сети с компьютеров и мобильных устройств с подключением к интернету вне дома. Подключения разрешены [пользователям системы](#) с правом доступа "vpn". Для доступа клиентов VPN-сервера в Интернет необходимо включить опцию "Транслировать адреса клиентов (NAT)".

Включить: ☒

Одно подключение на пользователя: ☒

Разрешить подключения без шифрования: ☐

Транслировать адреса клиентов (NAT): ☐

Доступ к сети: [Home network \(Wired and wireless hosts\) \(Home\)](#)

Начальный адрес пула:

Размер пула адресов:

Имя пользователя	IP-адрес	Доступ разрешен
admin	Авто	Нет

Рисунок 2.24. Настройка VPN-сервера

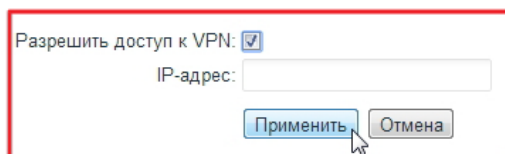


Рисунок 2.25. Настройка VPN-сервера

Настройка подключения к VPN-серверу интернет-центра для доступа к удаленной локальной сети представлена на рисунках 2.26, 2.27.

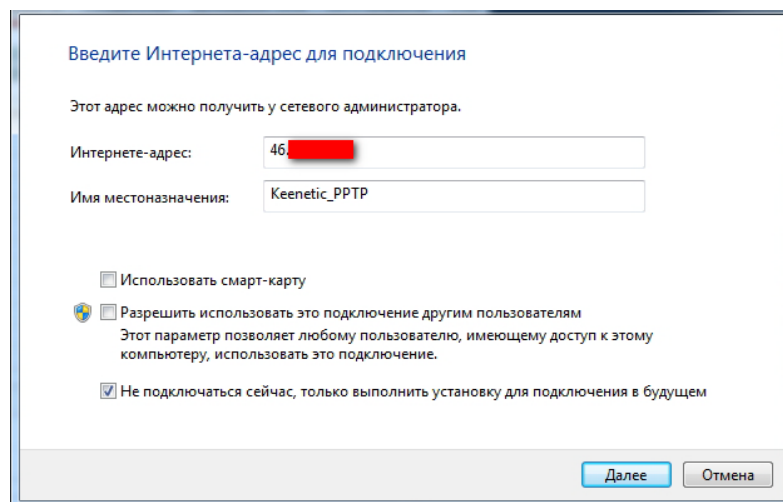


Рисунок 2.26. Настройка подключения к VPN-серверу

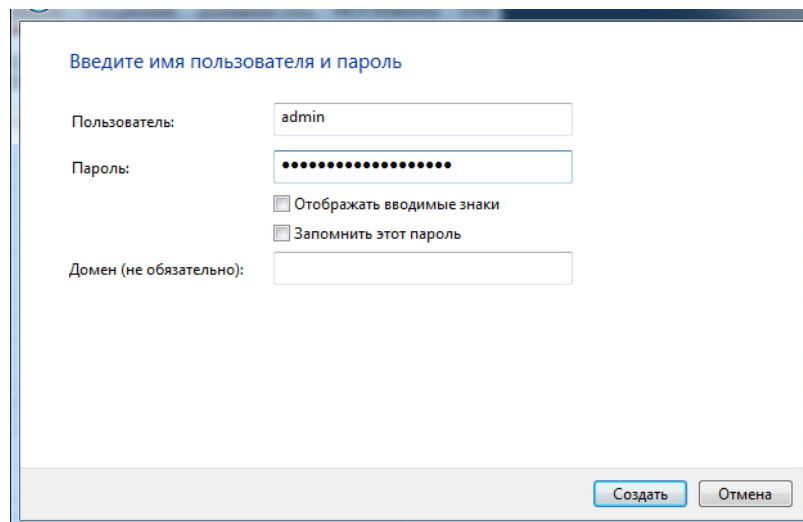


Рисунок 2.27. Настройка подключения к VPN-серверу

После создания VPN-подключения для сокращения времени подключения к серверу можно зайти в меню Центр управления сетями и общим доступом > Изменения параметров адаптера, найти созданное подключение, щелкнуть по нему правой кнопкой мыши, зайти в Свойства >

Безопасность > Тип VPN и принудительно установить Туннельный протокол точка-точка (PPTP). После этих настроек можно производить VPN-подключение. Клиент подключится и получит IP-адрес из указанного пула IP-адресов. Рисунок 2.28.

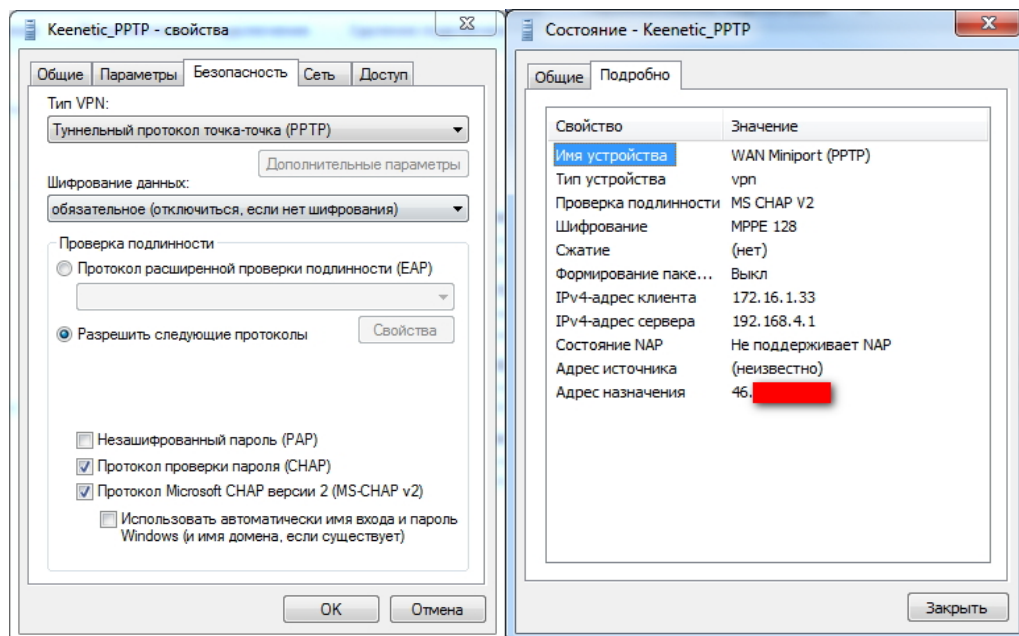


Рисунок 2.28. Настройка VPN-соединения на рабочем месте

Для защиты от несанкционированного доступа к компьютеру управляющего, применяется в организации политика локальных учетных данных. Логин и пароль для входа в ПК знает только управляющий ресторана.

Защиту от возможных вирусных атак обеспечивает Kaspersky Internet Security. Система включает в себя такие функции как:

- защита от вредоносного ПО;
- защита от взлома устройств злоумышленниками;
- шифрование истории браузера и онлайн-данных, а также блокирование приложений для слежки через веб-камеру и программ-шпионов;
- функции для защиты домашней сети Wi-Fi и периферийных устройств.

Важной составляющей в организации системы комплексной защиты

ресторана быстрого питания, является защита платежных операций и личных данных клиентов ресторана, а также ведение бухгалтерского учета с отправкой отчетности в головной офис сети ресторанов «Макдоналдс». Данная функция возлагается на следующую структуру, представленную на рисунке 2.29.



Рисунок 2.29. Принципиальная схема организации защиты платежей в ресторане быстрого питания

Платежные данные посетителей шифруются на самих терминалах средствами той организации или банка, который занимается обслуживанием этих терминалов. Далее информация со всех терминалов поступает в локальную базу данных под управлением системы 1С:Предприятие 8. Фастфуд. Все необходимые отчеты закрепляются неквалифицированной электронной подписью и отправляются в головной офис, т.е. базу данных и в банк, который обслуживает данный ресторан. В конце смены осуществляется сверка операций платежных терминалов с локальной базой данных. В случае совпадения информации общий итоговый отчет закрепляется ЭЦП и направляется в головной офис. Благодаря данной системе можно быть уверенным, что данные посетителей и коммерческая информация ресторана, надежно защищены.

2.4. Применяемые охранные и пожарно-охранные средства

Так как ресторан быстрого питания располагается на территории

торгового центра, то пожарно-охранная система полностью зависит и сопряжена с общей пожарно-охранной системой всего торгового центра.

В данной дипломной работе возможно только декларирование технических средств, применяемых для защиты от пожара и проникновения, которые установлены в общей системе торгового центра.

В качестве противопожарной системы применяются следующие компоненты:

- датчики дыма Рубеж – срабатывают при первых признаках задымления;
- датчики газа Rubetek - являются необходимым прибором для проверки утечек газа на кухне и в любом другом помещении;
- сирены для охранно-пожарных систем 31 ВЕК – оповещение при пожаре звуковое и световое;
- кнопки пожарной сигнализации Рубеж – позволяют сотрудникам и посетителям вручную подать сигнал об опасности;
- табличка «Выход» - фотолюминесцентное покрытие позволяет табличке светиться в темноте;
- система удаления дыма (СДУ) - это технологическое оборудование приточно-вытяжной вентиляции, создающее подпор воздуха и удаления продуктов горения, с целью создания условий для эвакуации людей при пожаре;
- углекислотный огнетушитель Ярпожинвест ОУ-3 – располагается в помещении кухни ресторана, на случай борьбы с небольшим локальным возгоранием (2 штуки).

В качестве организации системы борьбы с несанкционированным проникновением в помещения торгового центра, применяется следующее оборудование:

- внешнее видеонаблюдение – позволяет вести круглосуточную запись событий по периметру торгового центра;

- датчики движения Hikvision - снабжены PIR-сенсором для детекции перемещения человека в зоне радиусом до 10 м;
- датчики открытия двери/окна Hikvision - предназначены для контроля состояния двери или окна;
- датчики разбития стекла Ajax - детектируют разбитие стекла электретным микрофоном, фиксирующим сопровождающие процесс специфические звуки.

Комплексная работа всех систем позволяет гарантировать безопасность посетителей, сотрудников и имущества ресторана быстрого питания.

2.5. Рекомендации по усовершенствованию комплексной системы безопасности ресторана быстрого питания

Для повышения уровня безопасности в рассматриваемом в данной дипломной работе ресторана быстрого питания, является возможным сформулировать несколько рекомендаций по усовершенствованию комплексной системы безопасности.

Первое, организовать радиосвязь между сотрудниками ресторана. Реализация данной системы позволит решить такие задачи как:

- сотрудники ресторана смогут оперативно связываться друг с другом как при деловых контактах, так и в экстренной ситуации;
- руководство может следить за тем, как осуществляется процесс общения сотрудников с посетителями, для повышения уровня обслуживания клиентов;
- повышение самодисциплины сотрудников;
- возможность прослушивания записей при возникновении внештатных или конфликтных ситуаций.

Второе, включить в штат сотрудников ресторана электрика - каждое утро он обязан проходить по вверенной ему территории для выявления неисправностей. Составлять акт и незамедлительно устранять, блокировать

или отключать оборудование до устранения неполадок.

Третье, проводить обучение сотрудников ресторана действиям при возникновении чрезвычайных ситуаций. Они должны уметь организовать эвакуацию как посетителей ресторана, так и самих себя. Знать, где располагаются кнопки пожарной сигнализации, как пользоваться огнетушителями.

Четвертое, перевести все технические средства защиты помещений и ограничения доступа на биометрические. Это является более современным и технологически совершенным способом организации защиты. Пароли и ключи можно забыть, потерять, передать другому лицу, а с биометрическими данными этого сделать невозможно.

Пятое, установить в помещениях ресторана систему автоматического пожаротушения. Это может быть водяная, порошковая или газовая система. Ее установка позволит в автоматическом режиме и в максимально короткое время потушить пожар, не ждать приезда пожарных, не дать огню разгореться и уничтожить материально-техническую базу ресторана и нанести вред здоровью посетителей и персонала.

ЗАКЛЮЧЕНИЕ

В данной дипломной работе был рассмотрен вопрос организации системы комплексной безопасности в ресторане быстрого питания.

Во время исследования было выяснено, что для организации комплексной системы защиты ресторана необходимо организовать систему видеонаблюдения, систему пожаротушения, систему защиты от проникновения, систему защиты платежной и личной информации, систему защиты компьютерного и коммуникационного оборудования. Все эти системы, работая вместе и согласовано, позволяют организовать достаточно высокий уровень комплексной защиты ресторана быстрого питания от возможных угроз.

Предметом исследования выступали методы и средства, используемые на практике, которые позволяют обеспечить комплексную защиту ресторана быстрого питания.

Целью данной работы являлось рассмотрение существующих и применяемых методов и средств комплексной защиты, а именно основных вопросов и понятий защиты и безопасности, видов угроз безопасности, не только программных, физических, но и правовых методов и средств обеспечения комплексной защиты. Необходимо было рассмотреть и конкретные вопросы программной защиты информации в корпоративных сетях, существующие программные решения в этой области.

Для достижения поставленной цели были решены следующие задачи:

- проанализирована необходимость организации комплексной защиты ресторана;
- исследованы внешние и внутренние угрозы объекта защиты;
- оценены перспективные решения в сфере обеспечения комплексной безопасности;
- разработаны рекомендации и предложения по совершенствованию комплексной системы защиты;

- изучены существующие конкретные средства и методы комплексной защиты.

Результатом данной дипломной работы является полный набор конкретных средств и методов организации комплексной защиты ресторана быстрого питания. Обоснован выбор оборудования, технических и программных средств защиты. Уделено внимание документационному обеспечению деятельности организации. Разработаны конкретные рекомендации по усовершенствованию комплексной системы защиты ресторана быстрого питания.

Все задачи дипломной работы выполнены. Цель дипломной работы достигнута.

БИБЛИОГРАФИЯ

I. Научная литература и материалы периодической печати

1. Баранова Е., Бабаш А. Информационная безопасность и защита информации Издательский центр «Академия», 2019. — 374 с.;
2. Вихорев, С. Как определить источники угроз/Открытые системы. – 2018. - №07-08, 443с.;
3. Гафнер, В.В. Информационная безопасность: Учебное пособие - Рн/Д: Феникс, 2019. - 324 с.;
4. Грибунин В. Г., Чудовский В.В. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений — М. : Издательский центр «Академия», 2018. — 416 с.;
5. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие - Ст. Оскол: ТНТ, 2019. - 384 с.;
6. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности, – СПб: СПбНИУИТМО, 2018. – 173с.;
7. Конахович Г. Защита информации в телекоммуникационных системах/- М.:МК-Пресс,2018.- 356с.;
8. Михеева Е.В. Информационные технологии в профессиональной деятельности: учеб. пособие для студ. сред. проф. образования / - 8-е изд., стер. – М.: Издательский центр «Академия», 2019. – 384с.
9. Осмоловский С. А. Стохастические методы защиты информации/– М., Радио и связь, 2020. – 187с.;
- 10.Семенов Г. Цифровая подпись. // Открытые системы. – 2019. №07-08. 278с.;
- 11.Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий. – М.: Радио и связь, 2018, 128с.

II. Интернет-ресурсы

1. <https://kiosks.ru/index.php/product/onlajn-kassa-yarus-m2100f/>
2. <https://kiosks.ru/index.php/product/avtomaticheskaya-kassa-pos-monoblok-mikromarket/>

3. <https://izion.pro/kaluga/fire-alarm>
4. <https://www.dssl.ru/>
5. <https://habr.com/ru/company/dsec/blog/347432/>
6. <https://www.anti-malware.ru/threats/POS-hacking>
7. <https://solutions.1c.ru/catalog/fastfood/features>
8. <https://yunso.ru/elektronnye-zamki?https://yunso.ru/audioregistratory-osa&https://yunso.ru/audioregistratory-osa&yclid=2162785693879272298&https://skud-new.ru>
9. <https://kaluga.oknamydom.ru/plastikovie-dveri/>
10. <https://www.hrobot.ru/>
11. <https://ru.ivideon.com/videonablyudenie>
12. <https://www.kaspersky.ru>
13. <https://kontur.ru/press/news/company/2019/11/6862>
14. <https://www.business.ru/article/2504-elektronnaya-podpis-dlya-yuridicheskikh-lits>
15. https://video-praktik.ru/datchiki_pozharnye_knopki.html