

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования

**«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему Разработка защищенной ТКС предприятия общественного питания

Исполнитель Коротков Максим Дмитриевич

(фамилия, имя, отчество)

Руководитель Доктор технических наук, профессор

(ученая степень, ученое звание)

Фомин Владимир Владимирович

(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____

(подпись)

профессор, доктор технических наук

(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич

(фамилия, имя, отчество)

«17» февраля 2017 г.

Санкт-Петербург

2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение

высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему Разработка защищенной ТКС предприятия общественного питания

Исполнитель Коротков Максим Дмитриевич

(фамилия, имя, отчество)

Руководитель Доктор технических наук, профессор

(ученая степень, ученое звание)

Фомин Владимир Владимирович

(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____

(подпись)

профессор, доктор технических наук

(ученая степень, ученое звание)

Бурлов Вячеслав Георгиевич

(фамилия, имя, отчество)

«__» _____ 20__ г.

Санкт–Петербург

2017

РЕФЕРАТ

Отчет 73 с., 4 г., 34 рис., 30 источников, 2 прил.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ,
ГОЛОСОВАЯ БИОМЕТРИЯ, ОБРАБОТКА СИГНАЛА, ГАУССОВЫ
СМЕСИ.

Объектом исследования является анализ и сравнение систем и методов защиты информации в сфере общественного питания.

Цель работы — проектирование для достижения конкурентных преимуществ.

В процессе работы реализовывался современный подход к решению цели.

Задачи, которые необходимо решить в работе для достижения цели :

- Анализ и применение новых технологий
- Проектирование сетей
- Анализ и выбор программного решения для сотрудников

В работе был проведен полный обзор предметной области и реализованы поставленные задачи.

Было установлено, что с экономической точки зрения, устанавливая комплексную систему защиты на предприятия, главным фактором является сбор актуальных предложения, для решения разноплановых задач.

Оглавление:

Введение	4
1. Анализ и применение новых технологий	6
2. Обоснование необходимости выполнения проекта	8
2.1.1 Обоснование организации Wi-Fi сети в ресторане	8
2.1.2 Частотные полосы и каналы в Wi-Fi	8
2.1.3 Обоснование организации видеонаблюдения в ресторане	11
2.1.4 Общая часть	12
2.1.5 Требование к прокладке кабельных линий.	13
2.2 Общие сведения	15
2.3 Выбор оборудования	16
2.3.1 Сравнение камер	24
2.4 Безопасность беспроводных сетей Wi-Fi	29
2.4.1 Основные стандарты и протоколы безопасности	29
2.4.2 Проектирование Wi-Fi сети и видеонаблюдения.	33
2.5 Выбор программного обеспечения и оборудования для работников зала.	34
3. Проектная часть	48
3.1 Проектирование wi-fi сети	48
3.2 Проверка расчетов программы	53
3.3 Определение количества точек доступа для выбранного помещения	54
3.4 Проектирование видеонаблюдения и рабочей сети	56
3.5 Сеть	68
3.6 Вход в ресторан	70
4. Опасные и вредные факторы при работе с ЭВМ	72
4.1 Требования к работе в помещениях с ЭВМ	75
4.2 Требования к рабочему месту оператора	79
Заключение	84
Список литературы	85

Актуальность

В последнее время вырос интерес к вопросам защиты информации. Это связывают с тем, что стали более широко использоваться вычислительные сети, что приводит к тому, что появляются большие возможности для несанкционированного доступа к передаваемой информации.

Актуальность проблемы защиты информации связана с ростом возможностей вычислительной техники. Развитие средств, методов и форм автоматизации процессов обработки информации, массовость применения ПЭВМ резко повышают уязвимость информации. Поэтому, в настоящее время во всем мире в быстром темпе растет потребность в комплексных решениях по защите информации, особенно в сфере бизнеса.

Цель работы: Целью является проектирование для достижения конкурентных преимуществ.

В результате должен быть составлен набор документов, отвечающих известным требованиям и достаточных для начала работ по реализации предлагаемых решений. Для достижения этой цели необходимо решить ряд конкретных задач, значительная часть которых связана с разработкой системного проекта

В соответствии с целью были определены следующие задачи:

1. Анализ и применение новых технологий
2. Проектирование сетей (локальная сеть, wi-fi сеть, сеть видеонаблюдения)
3. Анализ и выбор программного решения для сотрудников

Введение

Традиционные средства защиты (антивирусы, фаерволы и т.д.) на сегодняшний день не способны эффективно противостоять современным киберпреступникам. Для защиты информационной системы организации требуется комплексный подход, сочетающий несколько рубежей защиты с применением разных технологий безопасности.

Для защиты от внешних угроз безопасности в Интернете хорошо зарекомендовывала себя система предотвращения вторжений на уровне хоста (HIPS). Правильно настроенная система обеспечивает беспрецедентный уровень безопасности, близкой к 100%. Правильно разработанные политики безопасности, а также с использованием HIPS других средств защиты данных программного обеспечения (например, антивирусный пакет) обеспечивают очень высокий уровень безопасности. Организация получает защиту от почти всех видов вредоносных программ, что значительно усложняет работу хакера, который решил попробовать преодолеть защиты предприятия, что сохраняет интеллектуальную собственность и критическую организацию данных.

Защита от внутренних угроз также требует комплексного подхода. Она выражается в разработке надлежащей политики информационной безопасности, внедрение четкой организационной структуры, несущей ответственность за безопасность сотрудников, контроль документооборота, контроля и мониторинга пользователей, внедрение передовых механизмов аутентификации для доступа к информации разной степени важности. Степень такой защиты зависит от объективных потребностей организации защиты информации. Не все объекты требуют дорогостоящих DLP-систем, которая дает хорошие результаты для защиты утечки корпоративных данных, но требуют сложных процедур для осуществления и обзора существующих механизмов рабочего процесса. Лучший выбор для большинства компаний станет внедрение функциональной защиты от утечки данных, контроль

документов и мониторинг действия пользователей локальной сети. Это решение является недорогой, простой в установке и использовании, но очень эффективный инструмент для обеспечения информационной безопасности.

1. Анализ и применение новых технологий

Высокая конкурентоспособность оператора связи обычно достигается в том случае, когда проект модернизации телекоммуникационной сети является абсолютно устойчивым [5]. Это свойство присуще проектам, которые остаются эффективными при всех сценариях развития инфокоммуникационного рынка. Для разработки устойчивых проектов следует включить в привычный перечень анализируемых показателей ряд новых параметров, что неизбежно ведет к усложнению задач проектирования телекоммуникационных сетей.

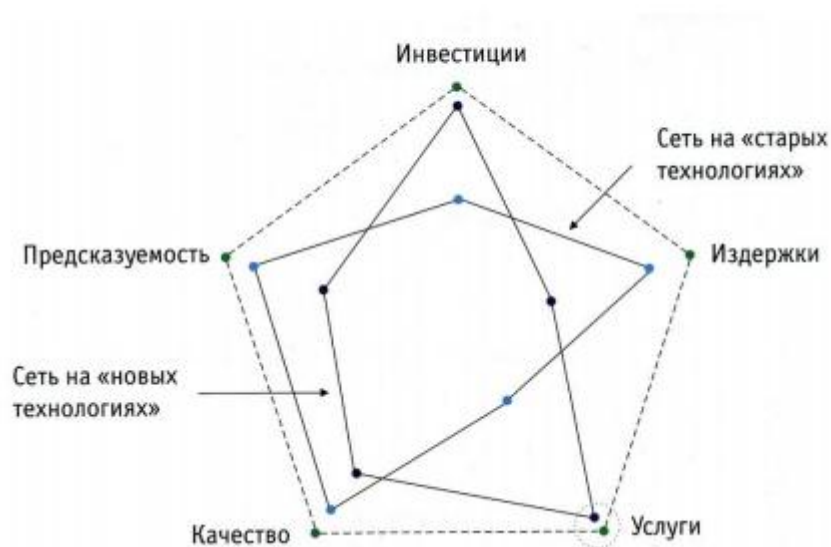


Рисунок 1. – Пример качественных оценок для двух сетей.

Любые новые технологии имеют неоспоримые плюсы, которые активно рекламируются их авторами и приверженцами. На этом фоне часто забывается, что практически любая новая технология имеет и отрицательные свойства. Пример качественных оценок для двух сетей, использующих старые и новые технологии, приведен на рис. 1 в виде трех

пятиугольников. Эти фигуры образованы путем соединения вершин, отражающих балльные оценки для выбранных пяти показателей телекоммуникационной сети.

Такой способ присвоения оценок обычно основан на том, что баллы находятся в диапазоне от нуля (минимум) до единицы (максимум).

Внешняя геометрическая фигура представляет собой правильный пятиугольник, который иллюстрирует некое гипотетическое решение: всем показателям присвоена максимальная оценка. Близость к максимальной оценке для сети, построенной на «старых технологиях», свойственна двум показателям: предсказуемости и качеству обслуживания. Утверждения такого рода в значительной мере объясняются опытом, накопленным операторами связи, производителями оборудования и проектными организациями. Вместе с тем большинству эксплуатируемых сетей свойственны два существенных недостатка: высокие издержки (эксплуатационные расходы) и ограниченный перечень поддерживаемых услуг.

Телекоммуникационные сети, основанные на «новых технологиях», поддерживают весьма широкий спектр услуг (на рис. 1 окружность, подчеркивающая близость соответствующей балльной оценки к максимуму). Подобные функциональные возможности всегда связаны

с высокими инвестициями. Правда, при этом существенно сокращаются издержки оператора связи. Предсказуемость поведения сети, построенной на «новых технологиях», будет ниже из-за отсутствия опыта ее эксплуатации. Серьезный недостаток пакетных технологий заключается в возможности снижения ряда показателей качества обслуживания [7].

Следовательно, для эффективного применения новых технологий необходимо найти подходящие системно-сетевые решения. Разработка подобных решений, как правило, не может быть сведена к задачам, которые решаются экономико-математическими методами.

2. Обоснование необходимости выполнения проекта

2.1.1 Обоснование организации Wi-Fi сети в ресторане.

Необходимость сети Wi-Fi состоит в том, что для гостей ресторана и сотрудников необходим выход в Интернет. В свою очередь сотрудникам нужно организовать доступ к общим сетевым ресурсам (общие хранилища, документы, принтеры и т.д.). Возникают случаи, когда необходимо выйти в сеть Интернет не только с компьютера или ноутбука, но и с портативных устройств, которые позволяют оптимизировать рабочий процесс за счет средств современных сетевых инфраструктур – видеоконференций, IP-телефонии, электронной почты, управления серверами и сетевыми устройствами.

Высокий уровень безопасности Wi-Fi говорит о его преимуществах при использовании на предприятиях, где безопасность информации один из главных критериев сети. В Wi-Fi применяются сложные методы шифрования.

2.1.2 Частотные полосы и каналы в Wi-Fi

Используемые частоты и каналы в диапазоне 2,4 ГГц

Для беспроводной Wi-Fi связи используется определенный диапазон частот, причем в зависимости от страны, этот диапазон может быть различным. Весь диапазон частот разбит на несколько каналов, на которых может работать оборудование. Стандарты 802.11b, 802.11g и 802.11n определяют следующие каналы таблица 1:

Таблица 1 – Используемые частоты и каналы в диапазоне 2,4 ГГц

Канал	Центральная частота	Страны
1	2.412	США, Европа, Российская Федерация, Япония
2	2.417	США, Европа, Российская Федерация, Япония
3	2.422	США, Европа, Российская Федерация, Япония
4	2.427	США, Европа, Российская Федерация, Япония
5	2.432	США, Европа, Российская Федерация, Япония
6	2.437	США, Европа, Российская Федерация, Япония
7	2.442	США, Европа, Российская Федерация, Япония
8	2.447	США, Европа, Российская Федерация, Япония
9	2.452	США, Европа, Российская Федерация, Япония
10	2.457	США, Европа, Российская Федерация, Япония
11	2.462	Европа, Российская Федерация, Япония
12	2.467	Европа, Российская Федерация, Япония
13	2.472	Япония

Из таблицы 1 видно, что шаг каналов в диапазоне 2,4 ГГц составляет 5 МГц, а ширина канала, как описано выше, составляет 20МГц. Таким образом, спектр рабочих частот оборудования перекрывается и независимых каналов, работа на которых возможна без взаимных помех, всего три – например 1 (2,412 ГГц), 6 (2,437 ГГц) и 11 (2,462 ГГц), частоты которых отличаются более чем на 20 МГц. Можно также использовать как независимые каналы 2, 7, 12 или 3, 8, 13.

Используемые частоты и каналы в диапазоне 5 ГГц

Частотные полосы и каналы для 5 ГГц:

UNII-1: 5150 – 5250 МГц (доступно 4 частотных канала);

UNII-2: 5250 – 5350 МГц (доступно 4 частотных канала);

UNII-2 Extended: 5470 – 5725 МГц (доступно 11 частотных каналов);

UNII-3: 5725 – 5825 МГц (доступно 4 частотных канала).

Сетка рабочих каналов 5 ГГц приведена в таблице 2.

Таблица 2 – Частотные каналы в спектральной полосе 5GHz

Канал	Частота, ГГц	Канал	Частота, ГГц	Канал	Частота, ГГц	Канал	Частота, ГГц
34	5,17	62	5,31	149	5,745	177	5,885
36	5,18	64	5,32	15	5,755	180	5,905
38	5,19	100	5,5	152	5,76		
40	5,2	104	5,52	153	5,765		
42	5,21	108	5,54	155	5,775		
44	5,22	112	5,56	157	5,785		
46	5,23	116	5,58	159	5,795		
48	5,24	120	5,6	160	5,8		
50	5,25	124	5,62	161	5,805		
52	5,26	128	5,64	163	5,815		
54	5,27	132	5,66	165	5,825		
56	5,28	136	5,68	167	5,835		
58	5,29	140	5,7	171	5,855		
60	5,3	147	5,735	173	5,86		

Формирование каналов Wi-Fi в диапазоне 5 ГГц рисунок 2.

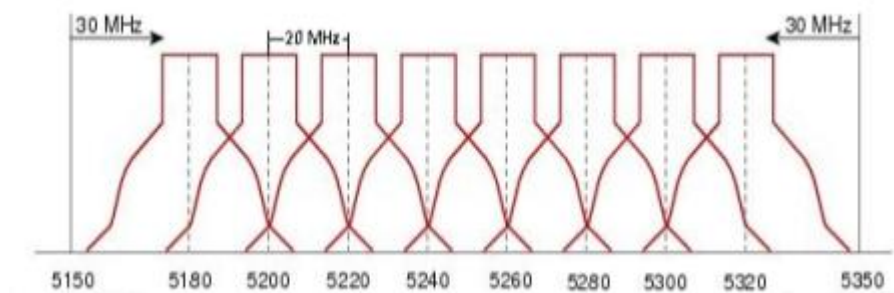


Рисунок 2 – Формирование каналов в диапазоне 5 ГГц

При этом дистанция от граничных диапазонов составляет 30 МГц, а межканальное разнесение составляет 20 МГц.

Из-за отсутствия использования и большого числа каналов точка Wi-Fi, скорость Wi-Fi увеличивается. Но необходимо использовать 5 ГГц, что бы не только Wi-Fi источник (маршрутизатор) работал на этой частоте, но и устройство (ноутбук, планшет, телефон, телевизор). Меньше использование 5GHz является высокая стоимость оборудования, по сравнению с устройствами, работающими на частоте 2,4 ГГц и меньшего радиуса действия по сравнению с частотой 2,4 ГГц.

2.1.3 Обоснование организации видеонаблюдения в ресторане.

В первую очередь видеонаблюдения предписано ведомственным нормативным актам.

“- объекты социально-культурного и коммунально-бытового назначения: здания учебно-воспитательного назначения, здравоохранения и социального обслуживания населения, сервисного обслуживания, здания и сооружения для культурно-досуговой деятельности и религиозных обрядов, временного проживания. Данные требования опосредованно вытекают из Приказа Минрегиона России от 05.07.2011 N 320 "Об утверждении свода правил "Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования" (вместе с СП 132.13330.2011

"Свод правил. Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования") и др."

2.1.4 Общая часть

Рабочий проект системы технологического видеонаблюдения и диспетчеризации, разработан для ресторана Квартира Кости Кройца.

Исходными данными для проектирования послужили следующие документы:

Техническое задание на выполнение работ по проектированию технологической системы видеонаблюдения и диспетчеризации в ресторане Квартира Кости Кройца.

Архитектурно-строительные чертежи.

Проект разработан в соответствии с действующими нормативно-техническими документами:

ГОСТР51558-2000. Системы охранные телевизионные. Общие технические требования и методы испытаний.

ОСТН-600-93 Отраслевые строительно-технологические нормы на монтаж сооружений и средств связи, радиовещания и телевидения

РД78.36.003-2002 Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств.

РД78.145-93 Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ.

РД78.36.004-2005 Рекомендации о техническом надзоре за выполнением проектных, монтажных и пусконаладочных работ по оборудованию объектов техническими средствами охраны.

Правила устройства электроустановок, изд.7, переработанное и дополненное, с изменениями.

СанПиН 2.2.2.542-96 Санитарные нормы и правила. Гигиенические

требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работ.

ГОСТ 12.1.030-81 ССБТ. Электробезопасность. Защитное заземление. Зануление (с Изм.1, утвержденным в марте 1987 года)

РД 78.36.002-99 Технические средства систем безопасности объектов. Обозначения условные графические элементов систем

ПП № 87 от 16.02.2008 г. «О составе разделов проектной документации и требования к их содержанию».

ГОСТ 31565-2012 Кабельные изделия. Требования пожарной безопасности.

СНиП 31-06-2009 Общественные здания и сооружения.

2.1.5 Требование к прокладке кабельных линий

Кабельные линии связи должны быть проложены в соответствии с согласованными сторонами схемами размещения на объекте системы безопасности.

Прокладку кабельных линий связи вести с учетом требований:

ВСН-600-81 - Инструкции по монтажу сооружений и устройств связи, радиовещания и телевидения;

РД 78.145-95 (ч.1, ч.2) - Пособие к руководящему документу “Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ”;

СНиП 3.05. 06 -85 - Электротехнические устройства;

ПУЭ - Правила устройства электроустановок.

ГОСТ 31565-2012 Кабельные изделия. Требования пожарной безопасности.

При прокладке кабелей системы следует соблюдать следующий порядок работ:

Произвести прокладку труб и кабелей, произвести разделку жил кабеля

и подключить их к оборудованию в соответствии с монтажными и электрическими схемами.

При прокладке кабелей не следует допускать повреждения внешней изоляции. Изгиб кабелей должен производиться с внутренним радиусом не менее $4d$ (d -диаметр внешней оболочки кабеля).

При прокладке кабеля к компонентам оборудования следует оставлять резерв на разделку не менее 5 метров для монтажного щита и для остального оборудования.

При параллельной прокладке слаботочных и силовых сетей расстояние в свету между ними не менее 300 мм.

При пересечении кабелей слаботочной сети с кабелями силовой сети, угол пересечения должен составлять 90 градусов.

Все электрические соединения выполняются с использованием клеммных колодок, либо пайкой. Скрутка кабеля не допустима.

В данном проекте используются кабельные изделия для одиночной прокладки, не распространяющие горения (кабель витая пара, кабель волоконно-оптический). Класс пожарной опасности – ПРГО2.

2.2 Общие сведения

Ресторан “Квартира Кости Кройца” расположенный в центральном районе города Санкт-Петербурга по адресу, г. Санкт-Петербург, Невский проспект 71 корпус 1. На 5 этаже здания.

Ресторан является условно-закрытым пространством.

Общая площадь ресторана составляет 900 кв.м.

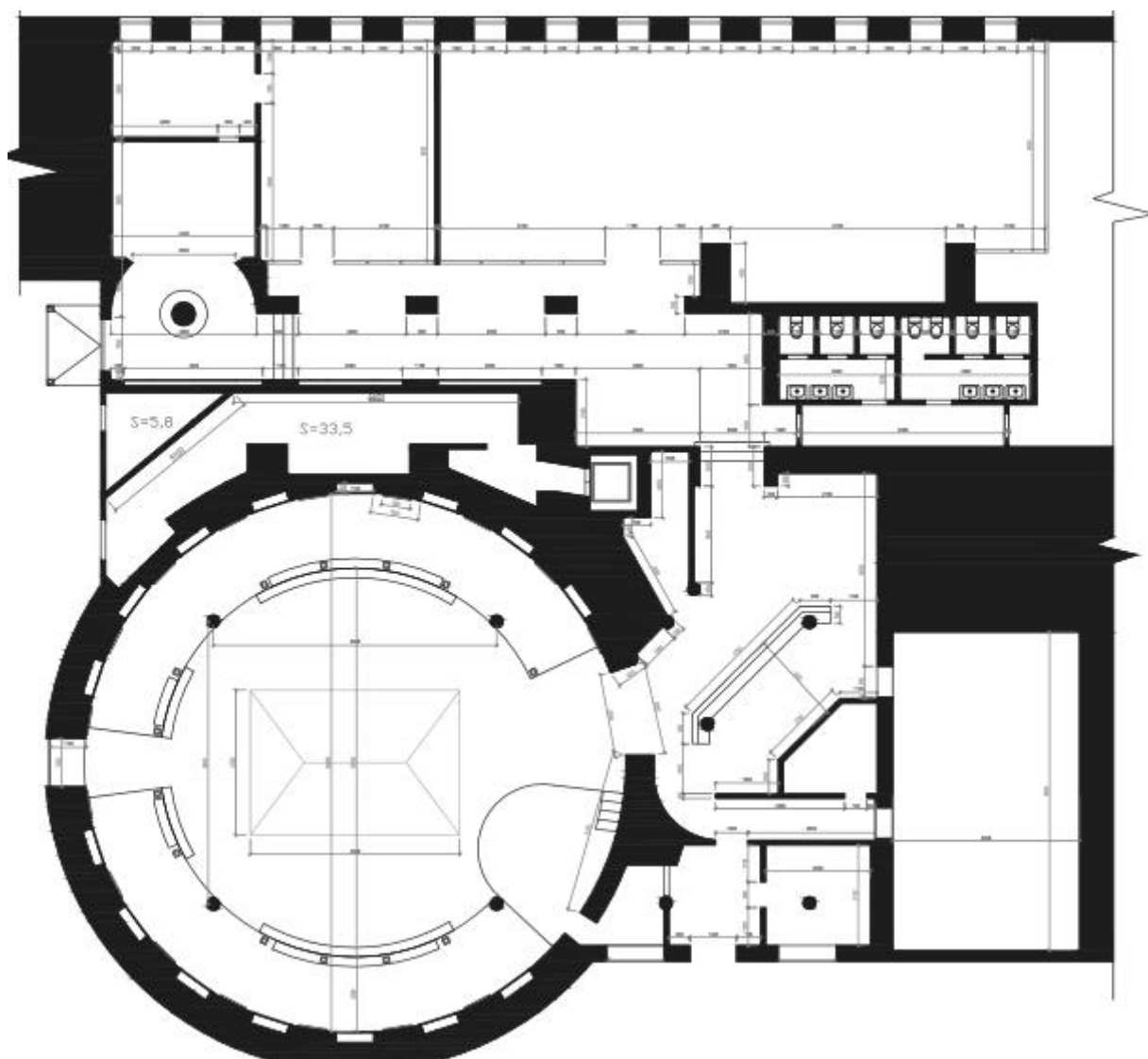


Рисунок 3 – План-схема ресторана.

На рисунке 3 показана план-схема заведения.

2.3 Выбор оборудования

DWL-3600AP – унифицированная точка доступа 802.11n Wi-Fi, разработанная для развертывания сетей бизнес-класса. Гибкая в управлении и поддерживающая передачу данных на высокой скорости, данная точка доступа обеспечивает легкую интеграцию в существующую сетевую инфраструктуру, которая в дальнейшем может быть расширена. Точка доступа может быть выполнена в корпусе класс Plenum (DWL-3600AP/A1A) или в обычном пластиковом корпусе (DWL-3600AP/A1A/PC)

Высокая производительность

Технология 2x2 MIMO обеспечивает передачу данных на скорости до 300 Мбит/с¹, используя частоту 2,4 ГГц. Помимо этого, точка доступа поддерживает технологию RadioProtect, благодаря использованию которой все пользователи получают обслуживание с высоким уровнем качества, даже в случае, если к сети подключены несколько пользователей, использующих устаревшие устройства стандартов 802.11b и 802.11g.

Безопасность

DWL-3600AP поддерживает новейшие стандарты безопасности, включая WPA, WPA2, и 802.1X. Помимо этого, DWL-3600AP поддерживает до 16 виртуальных точек доступа (VAP), что позволяет администратору назначать различные права доступа группам пользователей. Благодаря использованию унифицированных беспроводных коммутаторов D-Link можно увеличить уровень безопасности. Можно легко обнаружить в сети несанкционированные точки доступа, таким образом, администратор сможет немедленно предотвратить угрозу безопасности.

Quality of Service

DWL-3600AP поддерживает WMM, таким образом, в случае перегрузки сети, приоритет получит чувствительный ко времени трафик. Более того, если

несколько точек доступа DWL-3600AP находятся в непосредственной близости друг от друга, точка доступа будет отклонять новые запросы на подключение, так как все ресурсы используются. Вместо этого запрос на подключение будет принят соседней точкой доступа. Благодаря использованию данной функции ни одна точка доступа не будет перегружена, в то время как другие соседние точки доступа находятся в состоянии простоя.

Краткие характеристики DWL-3600AP

D-Link®

DWL-3600AP

Унифицированная точка доступа 802.11n

Технические характеристики

Система	Беспроводной интерфейс	802.11b/g/n 2,4 ГГц 2x2 MIMO	
	Интерфейс LAN	10/100/1000 Gigabit Ethernet	
	Консольный порт	RJ-45	
	Антенна	2 внутренних антенны	
	Коэффициент усиления антенны	4,7 dBi	
Питание		IEEE 802.3af Power Over Ethernet или внешний адаптер питания	
Диапазон частот	802.11b/g/n	2,4 - 2,4835 ГГц	
Скорость беспроводного соединения	802.11n	6,5 Мбит/с – 130 Мбит/с (20 МГц) 6,5 Мбит/с – 300 Мбит/с (40 МГц)	
	802.11g	54, 48, 36, 24, 18, 12, 9 и 6 Мбит/с	
	802.11b	11, 5,5, 2 и 1 Мбит/с	
Выходная мощность передатчика*	802.11b	21 dBm при 1 Мбит/с 21 dBm при 2 Мбит/с	21 dBm при 5,5 Мбит/с 21 dBm при 11 Мбит/с
	802.11g	21 dBm при 6 Мбит/с ~24 Мбит/с 19 dBm при 36 Мбит/с	18 dBm при 48 Мбит/с 17 dBm при 54 Мбит/с
	802.11n	2,4 ГГц/HT-20 20 dBm при MCS0/8 20 dBm при MCS1/9 20 dBm при MCS2/10 20 dBm при MCS3/11 19 dBm при MCS4/12 18 dBm при MCS5/13 17 dBm при MCS6/14 16 dBm при MCS7/15	2,4 ГГц/HT-40 19 dBm при MCS0/8 19 dBm при MCS1/9 19 dBm при MCS2/10 19 dBm при MCS3/11 17 dBm при MCS4/12 16 dBm при MCS5/13 14 dBm при MCS6/14 14 dBm при MCS7/15
	802.11b	-89 dBm при 2 Мбит/с -84 dBm при 11 Мбит/с	
	802.11g	-85 dBm при 6 Мбит/с -84 dBm при 9 Мбит/с -84 dBm при 12 Мбит/с -82 dBm при 18 Мбит/с	-78 dBm при 24 Мбит/с -73 dBm при 36 Мбит/с -70 dBm при 48 Мбит/с -68 dBm при 54 Мбит/с
Чувствительность приемника	802.11n	2,4 ГГц/HT-20 -82 dBm при MCS0/8 -79 dBm при MCS1/9 -77 dBm при MCS2/10 -74 dBm при MCS3/11 -70 dBm при MCS4/12 -66 dBm при MCS5/13 -65 dBm при MCS6/14 -64 dBm при MCS7/15	2,4 ГГц/HT-40 -79 dBm при MCS0/8 -76 dBm при MCS1/9 -74 dBm при MCS2/10 -71 dBm при MCS3/11 -67 dBm при MCS4/12 -63 dBm при MCS5/13 -62 dBm при MCS6/14 -61 dBm при MCS7/15

Рисунок 4.1 – Технические характеристики DWL-3600AP.

Цена = 11 000 рублей



Рисунок 1.3 – Точка доступа DWL-3600AP.

DWL-6600AP – унифицированная двухдиапазонная точка доступа 802.11n с поддержкой PoE для использования внутри помещений разработана для развертывания сетей бизнес-класса. Гибкая в управлении и поддерживающая передачу данных на высокой скорости, данная точка доступа обеспечивает легкую интеграцию в существующую сетевую инфраструктуру, которая в дальнейшем может быть расширена. Точка доступа может быть выполнена в корпусе класс Plenum (DWL-6600AP/A1A) или в обычном пластиковом корпусе (DWL-6600AP/A1A/PC).

Высокая производительность

DWL-6600AP обеспечивает передачу данных на скорости до 300 Мбит/с при частоте 2,4ГГц или 5ГГц. Поддержка функции Wi-Fi Multimedia™(WMM) делает точку доступа идеальным решением для аудио, видео и голосовых приложений. Кроме того, функция балансировки нагрузки

обеспечивает максимальную производительность и отличное качество обслуживания в беспроводной сети.

Автоматическая конфигурация кластера

Для небольших предприятий, которым требуется несколько точек доступа (ТД) и которые испытывают недостаток ресурсов, функция автоматической конфигурации кластера является идеальным решением. При установке небольшого количества точек доступа DWL-6600AP можно выполнить автоматическую конфигурацию кластера. После выполнения администратором настройки одной точки доступа, те же самые настройки будут применены к остальным точкам доступа. Таким образом, в кластер можно объединить до 16 точек доступа.

Унифицированное управление

DWL-6600AP может работать совместно с беспроводными коммутатором и контроллером D-Link. В этом режиме несколько точек доступа DWL-6600AP можно подключить напрямую или косвенно к одному из коммутаторов/контроллеров для обеспечения высокого уровня безопасности и беспроводной мобильности для беспроводных клиентов.

Безопасность

DWL-6600AP поддерживает новейшие стандарты безопасности Wi-Fi, включая WEP, WPA, WPA2 и 802.1X. Помимо этого, DWL-6600AP поддерживает до 16 виртуальных точек доступа (VAP) или до 32 в общей сложности), что позволяет администратору назначать различные права доступа для разным группам пользователей. Если включена функция «Изоляции станции», то точка доступа будет блокировать передачу данных между беспроводными клиентами, подключенными к беспроводной сети в одном радиочастотном диапазоне. Благодаря использованию унифицированных беспроводных коммутаторов D-Link можно увеличить

уровень безопасности. Можно легко обнаружить в сети несанкционированные точки доступа, таким образом, администратор сможет немедленно предотвратить угрозу безопасности.

Краткая характеристика DWL-6600AP

D-Link

DWL-6600AP

Унифицированная двухдиапазонная точка доступа 802.11n с поддержкой PoE

Технические характеристики

Система	Беспроводной интерфейс	802.11a/b/g/n 2,4/5 ГГц	
	Интерфейс LAN	10/100/1000 Gigabit Ethernet	
	Консольный порт	RJ-45	
	Антенна	встроенные пассивные всенаправленные 2x2 MIMO антенны для 2,4ГГц и 5ГГц, 4 коннектора RP-SMA для подключения внешних антенн	
	Коэффициент усиления антенны	5 dBi для 2,4ГГц и 6 dBi для 5ГГц	
	Питание	IEEE 802.3af Power Over Ethernet или внешний адаптер питания	
Частота	802.11n	2,4 ГГц – 2,497 ГГц и 4,9 ГГц – 5,85 ГГц	
	802.11b/g	2,4 ГГц – 2,485 ГГц	
	802.11a	5,15 ГГц – 5,35 ГГц и 5,725 ГГц – 5,825 ГГц	
Скорость беспроводного соединения	802.11n	6,5 Мбит/с – 130 Мбит/с (20 Мбит/с) 6,5 Мбит/с – 300 Мбит/с (40 Мбит/с)	
	802.11a/g	54, 48, 36, 24, 18, 12, 9 и 6 Мбит/с	
	802.11b	11, 5,5, 2 и 1 Мбит/с	
Выходная мощность передатчика*	802.11a/g	11 (+/-2) dBm при 54, 48, 36, 24, 18, 12, 9 и 6 Мбит/с	
	802.11b	13 (+/-2) dBm при 11, 5,5, 2 и 1 Мбит/с	
	802.11n	2,4 ГГц/HT-20 11 dBm при MCS0/8, MCS1/9, MCS2/10, MCS3/11, MCS4/12, MCS5/13, MCS6/14, MCS7/15	2,4 ГГц/HT-40 11 dBm при MCS0/8, MCS1/9, MCS2/10, MCS3/11, MCS4/12, MCS5/13, MCS6/14, MCS7/15
		5,0 ГГц/HT-20 11 dBm при MCS0/8, MCS1/9, MCS2/10, MCS3/11, MCS4/12, MCS5/13, MCS6/14, MCS7/15	5,0 ГГц/HT-40 11 dBm при MCS0/8, MCS1/9, MCS2/10, MCS3/11, MCS4/12, MCS5/13, MCS6/14, MCS7/15
Чувствительность приемника	802.11a	-86 (+/-2) dBm при 6 Мбит/с	-77 (+/-2) dBm при 24 Мбит/с
		-86 (+/-2) dBm при 9 Мбит/с	-75 (+/-2) dBm при 36 Мбит/с
		-84 (+/-2) dBm при 12 Мбит/с	-68 (+/-2) dBm при 48 Мбит/с
		-81 (+/-2) dBm при 18 Мбит/с	-67 (+/-2) dBm при 54 Мбит/с
	802.11b	-92 (+/-2) dBm при 1 Мбит/с	-88 (+/-2) dBm при 5,5 Мбит/с
		-90 (+/-2) dBm при 2 Мбит/с	-85 (+/-2) dBm при 11 Мбит/с
	802.11g	-87 (+/-2) dBm при 6 Мбит/с	-79 (+/-2) dBm при 24 Мбит/с
		-87 (+/-2) dBm при 9 Мбит/с	-76 (+/-2) dBm при 36 Мбит/с
		-85 (+/-2) dBm при 12 Мбит/с	-71 (+/-2) dBm при 48 Мбит/с
		-82 (+/-2) dBm при 18 Мбит/с	-67 (+/-2) dBm при 54 Мбит/с
	802.11n	2,4ГГц/HT-20 -85dBm при MCS0/8 -82dBm при MCS1/9 -80dBm при MCS2/10 -77dBm при MCS3/11 -74dBm при MCS4/12 -69dBm при MCS5/13 -68dBm при MCS6/14 -65dBm при MCS7/15	2,4ГГц/HT-40 -82 dBm при MCS0/8 -79 dBm при MCS1/9 -77 dBm при MCS2/10 -74 dBm при MCS3/11 -71 dBm при MCS4/12 -66 dBm при MCS5/13 -65 dBm при MCS6/14 -62 dBm при MCS7/15

Рисунок 4.2 - Технические характеристики DWL-6600AP.

Цена = 23 000 рублей



Рисунок 1.4 – Точка доступа DWL-6600AP.

DWL-2600AP

Описание:

Унифицированная однодиапазонная точка доступа DWL-2600AP с поддержкой PoE предназначена для использования внутри помещений и используется для построения сетей бизнес-класса. Удобная в управлении и поддерживающая высокую скорость передачи данных точка доступа DWL-2600AP обеспечивает легкую интеграцию в действующую сетевую инфраструктуру, которая может быть масштабирована в будущем в соответствии с требованиями пользователя.

Автоматическая конфигурация кластера

Функция автоматической конфигурации кластера является идеальным решением для предприятий малого бизнеса, которым требуется установить

несколько точек доступа (ТД) и которые испытывают недостаток ресурсов для решения задач сетевого управления. При установке небольшого количества точек доступа DWL-2600AP можно выполнить автоматическую конфигурацию кластера. После выполнения администратором настройки одной точки доступа, те же настройки будут применены к остальным точкам доступа. Таким образом, в кластер можно объединить до 8 точек доступа.

Унифицированное управление

При установке сети с использованием унифицированных беспроводных коммутаторов можно управлять до 192 точками доступа DWL-2600AP, таким образом, администратор может увеличить радиус действия беспроводной сети.

Безопасность

DWL-2600AP поддерживает новейшие стандарты безопасности, включая WPA и WPA2. Помимо этого, DWL-2600AP поддерживает до 16 SSID, что позволяет администратору назначать различные права доступа группам пользователей.

Автоматическая настройка частоты

При установке нескольких точек доступа на небольшом расстоянии друг от друга могут возникнуть помехи. При обнаружении соседнего узла точка доступа DWL-2600AP может автоматически выбрать канал без помех. Это значительно снижает помехи и позволяет администратору устанавливать точки доступа на близком расстоянии друг от друга. Если соседняя ТД работает на той же частоте, DWL-2600AP автоматически снижает мощность передачи¹. Если, по какой-либо причине соседняя ТД больше не действует в сети, DWL-2600AP увеличивает мощность передачи, чтобы увеличить радиус покрытия сети.

Quality of Service

DWL-2600AP поддерживает WMM, таким образом, в случае перегрузки сети, приоритет получит чувствительный ко времени трафик. Более того, если

несколько точек доступа DWL-2600AP находятся в непосредственной близости друг от друга, точка доступа будет отклонять новые запросы на подключение, так как все ресурсы используются. Вместо этого запрос на подключение будет принят соседней точкой доступа. Благодаря использованию данной функции ни одна точка доступа не будет перегружена, в то время как другие соседние точки доступа находятся в состоянии простоя.

Краткая характеристика DWL-2600AP

Технические характеристики			
Основное			
Беспроводной интерфейс	• 802.11b/g/n 2.4 ГГц		
Интерфейс LAN	• 10/100 Fast Ethernet		
Антенна	• Внутренняя антенна, 2X2 MIMO, коэффициент усиления 3 dBi		
Питание	• PoE или 12 В/1 А		
Функционал			
Частота	• 802.11b/g/n: 2.4 ГГц - 2,4835 ГГц		
Скорость беспроводного соединения	• 802.11n: 6,5 Мбит/с - 300 Мбит/с	• 802.11g: 54, 48, 36, 24, 12, 9 и 6 Мбит/с • 802.11b: 11, 5,5, 2 и 1 Мбит/с	
Выходная мощность передатчика*	• 802.11b: 21 dBm при 1 Мбит/с 19 dBm при 2 Мбит/с 17 dBm при 5,5 Мбит/с, 11 Мбит/с • 802.11g: 21 dBm при 6 Мбит/с ~18 Мбит/с, 19 dBm при 24 Мбит/с 18 dBm при 36 Мбит/с 17 dBm при 48 Мбит/с 15 dBm при 54 Мбит/с	• 802.11n(2,4 ГГц/HT-20): 20 dBm при MCS0/8 20 dBm при MCS1/9 20 dBm при MCS2/10 20 dBm при MCS3/11 19 dBm при MCS4/12 18 dBm при MCS5/13 17 dBm при MCS6/14 16 dBm при MCS7/15	• 802.11n(2,4 ГГц/HT-40) 19 dBm при MCS0/8 19 dBm при MCS1/9 19 dBm при MCS2/10 19 dBm при MCS3/11 17 dBm при MCS4/12 16 dBm при MCS5/13 14 dBm при MCS6/14 14 dBm при MCS7/15
Чувствительность приемника	• 802.11b: -89 dBm при 1 Мбит/с -89 dBm при 2 Мбит/с -84 dBm при 5,5 Мбит/с, 11 Мбит/с • 802.11g: -85 dBm при 6 Мбит/с -84 dBm при 9 Мбит/с -84 dBm при 12 Мбит/с -82 dBm при 18 Мбит/с -78 dBm при 24 Мбит/с -73 dBm при 36 Мбит/с -70 dBm при 48 Мбит/с -68 dBm при 54 Мбит/с	• 802.11n (2,4ГГц/HT-20): – 82dBm при MCS0/8 – 79dBm при MCS1/9 – 77dBm при MCS2/10 – 74dBm при MCS3/11 – 70dBm при MCS4/12 – 66dBm при MCS5/13 – 65dBm при MCS6/14 – 64dBm при MCS7/15	• 802.11n (2,4ГГц/HT-40) -79 dBm при MCS0/8 -76 dBm при MCS1/9 -74 dBm при MCS2/10 -71 dBm при MCS3/11 -67 dBm при MCS4/12 -63 dBm при MCS5/13 -62 dBm при MCS6/14 -61 dBm при MCS7/15
Web-интерфейс пользователя	• HTTP/HTTPS		
Интерфейс командной строки	• Консольный порт с RJ45 разъемом • Telnet/ SSH		• SNMP
Безопасность			
SSID	• 16 SSID • 802.1Q VLAN		• Изоляция станции
Защита беспроводной сети	• WPA Personal/ Enterprise		• WPA2 Personal/ Enterprise
Обнаружение и предотвращение	• Классификация авторизованных и неавторизованных точек доступа		
Аутентификация	• Фильтрация по MAC-адресам		
Физические характеристики			
Размеры	• 160 x 160 x 45 мм		
Вес	• 240 г		
Адаптер питания	• от 100 до 240 В переменного тока		• Выходная мощность: 12 В постоянного тока, 1 А
Power over Ethernet	• 10/100 Мбит/с PoE (802.3af)		
Корпус	• Стандартный или класса «Plenum»		
Температура	• Рабочая: от 0 до 40 °C		
Влажность	• Рабочая: от 10% до 90% (без конденсата)		
Сертификаты	• CE • FCC • IC • cUL • LVD • UL 2043 (только для класса «Plenum»)		• C-Tick • VCCI • NCC • Wi-Fi • TELECOM

Рисунок 4.3 – Технические характеристики DWL-2600AP.

Цена = 6000 рублей



Рисунок 1.5 - Точка доступа DWL-2600AP.

Итог

В соотношении цена-качество идеальным решением для нашей задачи подходит DWL-3600AP.

2.3.1 Сравнение камер

Рассмотри 2 камеры от того

Таблица 2



производителя D

ление видео



Модель	DCS-2230	DCS-2230L
Характеристики видео		
Кодеки сжатия	H.264, MPEG-4, MJPEG	H.264, MPEG-4, MJPEG
Максимальное разрешение	2 мегапиксельный (Full HD)	2 мегапиксельный (Full HD)

Разрешение @ кадров/сек (16:9)	1920x1080 @ 15кадров/сек 1280x720 @ 30кадров/сек	1920x1080 @ 30кадров/сек 1280x720 @ 30кадров/сек 800x450 @ 30кадров/сек 640x360 @ 30кадров/сек 480x270 @ 30кадров/сек 320x176 @ 30кадров/сек 176x144 @ 30кадров/сек
Разрешение @ кадров/сек (4:3)	1280x800 @ 30кадров/сек 640x480 @ 30кадров/сек 320x240 @ 30кадров/сек 176x144 @ 30кадров/сек	1440x1080 @ 30кадров/сек 1280x960 @ 30кадров/сек 1024x768 @ 30кадров/сек 800x600 @ 30кадров/сек 600x480 @ 30кадров/сек 480x360 @ 30кадров/сек 320x240 @ 30кадров/сек 176x144 @ 30кадров/сек
Битрейт видео	64kbps ~ 8Mbps	64kbps ~ 8Mbps
Широкий динамический диапазон (WDR)	нет	нет
Автоматический баланс белого (AWB)	да	да
Количество приватных масок	3 зоны	3 зоны
Переворот и отражение	да	да
Характеристики объектива		
Сенсор	1/2.7" 2 мегапиксельный CMOS сенсор с прогрессивной разверткой	1/2.7" 2 мегапиксельный CMOS сенсор с прогрессивной разверткой
ICR	ICR фильтр	ICR фильтр
ИК подсветка (расстояние)	ИК подсветка 5 метров	ИК подсветка 5 метров
Минимальная освещенность	1 Lux (цветной) 0 Lux (Ч/Б, при вкл. ИК подсветке)	1 Lux (цветной) 0 Lux (Ч/Б, при вкл. ИК подсветке)
Аппертура (число F)	F2.0	F1.8

Объектив	фиксированный фокус	фиксированный фокус
Фокусное расстояние	4.37мм	2.8мм
Оптическое увеличение	нет	нет
Угол обзора (горизонтальный/верт икальный)	67.4° / 40.8°	103° / 55°
Характеристики ePTZ(цифровое)		
Цифровое увеличение	10x	10x
Цифровой PTZ (ePTZ)	да	да
Характеристики аудио		
Двухсторонняя связь	да	да
Встроенный микрофон	да	да
Встроенный динамик	да	да
Аудиовход	нет	нет
Аудиовыход	нет	нет
Выключение звука	да	да
Детектор звука	нет	нет
Характеристики обработки событий		
Детектор движения	да	да
Обнаружение воздействия на корпус	нет	нет
PIR сенсор	да	да
Запись по событию	да	да
Уведомление по email	да	да
Характеристики		

записи		
Запись на сетевой ресурс (самба клиент)	да	да
Поддержка карт памяти	Micro SD (макс. 32GB)	Micro SD (макс. 32GB)
Сетевые протоколы		
NTP	да	да
SMTP	да	да
FTP	да	да
RTSP	да rtsp://ip адрес:порт/live1.sdp	да rtsp://ip адрес:порт/live1.sdp
ONVIF	да	да
Сервис mydlink		
Поддержка сервиса mydlink	нет	да
Сетевые соединения		
LAN	10/100BASE-TX	10/100BASE-TX
WI-FI	802.11b/g/n	802.11b/g/n
Режим повторителя WI-FI сети	нет	нет
Физические характеристики		
Цифровой вход/выход (DI/DO)	1 / 1	1 / 1
Интерфейс RS-485	нет	нет
Аналоговый выход	нет	нет
Антивандаальный корпус	нет	нет
Питание	DC 5V	DC 5V
PoE	нет	нет

Максимальная потребляемая мощность	4.0 Вт	4.0 Вт
Рабочая температура	от 0 до 40°C	от 0 до 40°C
Размеры (ширина x длина x высота)	58 x 95 x 38.7 мм	58 X 38.7 X 95 мм
Вес	75 грамм	75 грамм

Одним из самых важных критериев в выборе камер было наличие веб интерфейса, и просмотра видео в реальном времени через приложение на телефоне, в следствии чего, выбор пал на DCS 2230L.

2.4 Безопасность беспроводных сетей Wi-Fi

2.4.1 Основные стандарты и протоколы безопасности

WEP

Первой технологией беспроводной безопасности считается протокол безопасности WEP (Wired Equivalent Privacy - Wired Equivalent безопасности), изначально заложены в стандартных 802.11. WEP. Протокол шифрования использует алгоритм RC4 нестабильную на статическом образом. Существует 64-, 128-, 256- и 512-битное шифрование. Чем больше количество бит, используемых для хранения ключа, тем больше возможных комбинаций ключа, и, соответственно, высокую устойчивость к растрескиванию сети. Часть WEP-ключ является статическим (в случае 40-битного 64-битного шифрования), а другая часть (24 бита) - динамическая (вектор инициализации), он изменяется во время работы сети. Основная уязвимость WEP является то, что векторы инициализации повторяются по истечении определенного периода времени, и злоумышленнику потребуется только обработать эти повторы и вычислить для них статическую часть ключа. Для повышения уровня безопасности можно в дополнение к WEP-шифрованием использования 802.1x или VPN стандарта. Особенности WEP – протокола:

- достаточно устойчив к атакам, связанных с простым перебором ключей шифрования, что обеспечивается необходимой длиной ключа и частотой смены ключей и инициализирующего вектора;
- самосинхронизация для каждого сообщения. Это свойство является ключевым для протоколов уровня доступа к среде передачи, где велико число искажений и потерянных пакетов;
- WEP легко реализовать;
- открытость;
- использование WEP – шифрования не является обязательным в сетях стандарта IEEE 802.11.

Таким образом, WEP технология не обеспечивает необходимый уровень безопасности корпоративной сети, но достаточно для домашней беспроводной сети, когда объем перехваченного сетевого трафика слишком мал для анализа и ключа открытия.

802.1X

IEEE 802.1X - это стандарт, который оказался решающим для развития отрасли беспроводной связи в целом. Он основан на исправлении недостатков технологий безопасности, применяемых в 802.11, в частности, возможность взлома WEP, в зависимости от производителя технологий и т.д. 802.1X позволяет подключать к сети даже PDA-устройства, что позволяет больше рычагов беспроводной коммуникация идея. С другой стороны, 802.1X и 802.11 совместимы. 802.1X использует тот же алгоритм, что и в WEP, а именно - RC4, но с некоторыми отличиями. 802.1X на основе Extensible Authentication Protocol Extensible Authentication Protocol (EAP), транспортный протокол уровня безопасности, Transport Layer Security (TLS) и сервер удаленного доступа RADIUS (Удаленный доступ пользователей по коммутируемым линиям сервера). Кроме того, стоит добавить новую организацию сетевых клиентов. После того как пользователь прошел этап аутентификации, его секретный ключ передается в зашифрованном виде в какой-то короткий промежуток времени - время для действий на момент сессии. По завершении этой сессии генерируется новый ключ, и снова отправляется пользователю. Протокол безопасности транспортного уровня TLS обеспечивает взаимную аутентификацию и целостность данных. Все клавиши 128-бит по умолчанию.

WPA

Протокол шифрования WPA. Сильнее протокол шифрования WEP, чем, хотя, используя тот же алгоритм RC4. Технология WPA предназначен для использования с сервером аутентификации 802.1X, который распределяет различные ключи для каждого пользователя. Тем не менее, он также может быть использован в менее безопасном режиме «Pre-Shared Key (PSK)». Ключ

PSK предназначен для домашних сетей и небольших офисных сетей, где все пользователи используют один и тот же пароль. Протокол WPA-PSK также называется WPA-Personal. Протокол WPA-PSK позволяет беспроводное устройство Brother для связи с точками доступа, используя метод шифрования TKIP или AES. Протокол WPA2-PSK позволяет беспроводное устройство Brother для связи с точками доступа, используя метод шифрования AES. TKIP (Temporal Key Integrity Protocol) - протокол динамической сети ключи, которые часто изменяются. TKIP несет ответственность за увеличение от 40 до 128-битного размера ключа, а также для замены статического ключа WEP, ключи автоматически генерируются и отправляются на сервер аутентификации. Кроме того, TKIP использует специальную иерархию ключей и ключей методологии управления, которая удаляет излишнюю предсказуемость, которая была использована для несанкционированного снятия защиты ключей WEP. AES алгоритм (Advanced Encryption Standard) симметричный блочный алгоритм шифрования (размер блока 128 бит, ключ 128/192/256 битовых), принятый в качестве стандарта шифрования. AES является одним из наиболее распространенных алгоритмов симметричного шифрования.

Если в точке доступа используется протокол безопасности беспроводного доступа WPA-PSK, то на компьютере (адаптере) нужно использовать протоколы WPA и TKIP, а при использовании протокола WPA2-PSK на компьютере нужно использовать протокол WPA2 и стандарт AES. В противном случае пользователи не смогут подключиться к беспроводной точке доступа (невозможно подключиться к беспроводной точке доступа при использовании протокола WPA2 с протоколом TKIP).

Если точка доступа использует протокол безопасности беспроводной WPA-PSK, компьютер (адаптер) необходимо использовать протоколы WPA и TKIP, а также при использовании протокола WPA2-PSK на компьютере вы хотите использовать WPA2 и стандартный протокол AES. В противном случае пользователи не смогут подключиться к беспроводной точке доступа (вы не

можете подключиться к беспроводной точке доступа с использованием WPA2 с протоколом протокола TKIP). WPA2 - протокол защиты данных, который соответствует стандарту IEEE 802.11i для беспроводных локальных сетей с 2004 года более надежными, чем интервал, использовать протокол WPA, как для шифрования с помощью TKIP вместо гораздо более надежный алгоритм CCMP базируется на AES. С 2006 года все устройства с Wi-Fi логотип должен поддерживать WPA2. В отличие от WPA, WPA2 также хочет относительно новое оборудование, а это значит, что аппаратные средства приобретены, необходимо изменить до 2006. Там не две версии WPA2. Там WPA2 для корпоративных и домашних условий. Home Edition использует заранее этот ключ и проверяет, что это правильно сразу. Версия для предприятий делает это через сервер.

VPN

Технология виртуальной частной сети виртуальной частной сети (VPN) была предложена Intel, чтобы обеспечить безопасные клиентские системы соединения с серверами через общедоступные интернет-ссылки. VPN очень хорошо зарекомендовали себя с точки зрения шифрования класса и аутентификации. Плюс технология заключается в том, что в течение более трех лет практического применения в промышленности, протокол не получил каких-либо жалоб от пользователей. Информация о его взломе не было.

Технологий шифрования в VPN применяется несколько, наиболее популярные из них описаны протоколами PPTP, L2TP и IPSec с алгоритмами шифрования DES, Triple DES, AES и MD5. IP Security (IPSec) используется примерно в 65–70% случаев. С его помощью обеспечивается практически максимальная безопасность линии связи.

И хотя технология VPN не предназначалась изначально именно для Wi-Fi, она может использоваться для любого типа сетей, и идея защитить с её помощью беспроводные их варианты одна из лучших на сегодня.

Для реализации VPN-защиты в рамках сети необходимо установить специальный VPN-шлюз (программный или аппаратный), в котором

создаются туннели, по одному на каждого пользователя. Например, для беспроводных сетей шлюз следует установить непосредственно перед точкой доступа. А пользователям сети необходимо установить специальные клиентские программы, которые в свою очередь также работают за рамками беспроводной сети и расшифровка выносится за её пределы.

Хотя всё это достаточно громоздко, но очень надёжно, главный недостаток такого решения – необходимость в администрировании. Второй существенный минус – уменьшение пропускной способности канала на 30–40%.

2.4.3 Проектирование Wi-Fi сети и видеонаблюдения.

Для проектирования wifi сети и видеонаблюдения будут использоваться приложения компании Dlink: Wi-Fi Planner PRO и Surveillance Floor Planner PRO.

Оба приложения хороши тем, что автоматически рассчитывают энергопотребление оборудования, общую стоимость, wi-fi planner pro рассчитывает самое оптимальное месторасположения точек доступа.

2.5 Выбор программного обеспечения и оборудования для работников зала.

Было рассмотрено 3 вида программного обеспечения, разработанных специально для сферы общественного питания:

1. TillyPad XL v.9

Tillypad XL – это система автоматизации ресторана, кафе, бара, клуба, столовой или сети заведений общественного питания и развлекательных услуг. Tillypad XL поможет вам легко повысить эффективность своего заведения и увеличить свою прибыль!

Система Tillypad XL оптимизирует все бизнес-процессы: прием заказа, расчет с гостями, взаимодействие с кухней, программы лояльности, работу с меню, продуктами, товарами и рецептами, складской учет, работу с приходными и расходными документами, инвентаризацию, управление персоналом и контроль работы всего заведения. Вы легко и быстро получите все данные по продажам, себестоимости, прибыли, фудкосте, финансовые, маркетинговые и аналитические отчеты.

Надежность дома определяется фундаментом. Поэтому в основе Tillypad XL – SQL Server 2012, самая современная база данных компании Microsoft, серебряным партнером которой является Тиллипад. Tillypad XL – открытая система. Возможности её настройки и интеграции безграничны. Вся необходимая для этого информация есть на наших справочных ресурсах в интернете.

Tillypad XL – система для бизнеса любого масштаба. И начинающий ресторатор, и гигант индустрии получают быстрый запуск и полный контроль над своими заведениями. И всё это – вне зависимости от количества объектов и географии их расположения, пусть даже и в разных странах. С Tillypad XL центральный офис может устанавливать для всех заведений единые стандарты и следить за их неукоснительным соблюдением, ведущим ваш бизнес к успеху. Мы предлагаем уникальные возможности и выгодные условия для сетевых проектов и обладателей франшиз, стремящихся к глобальному росту и готовых модернизировать свой бизнес. [7]

Коммерческое предложение			
 RESTOCREATOR РЕСТОРАНЫ ПОД КЛЮЧ	Заказчик:		
	Исполнитель: ТехноИнжиниринг	Тел/факс	+7 (812) 611 11 62
	Контактные лица:	E-mail:	info@restocreator.ru
	Объект:	Сайт	http://www.restocreator.ru
Дата составления:		27.04.2016	
Стоимость проекта, руб.		1 094 025	
Права на использование программного обеспечения TillyPad XL v.9		263 000	
Серверное, торговое оборудование и офисные ПК		717 500	
Услуги		113 525	
Спецификация проекта	Стоимость, руб.	Кол-во, шт.	Сумма, руб.
Права на использование программного обеспечения TillyPad XL v.9			
ПО Tillypad XL Комплект F+F+BS	75000	2	150000
ПО Tillypad XL F	25000	1	25000
MS SQL 2012 64bit	12000	2	24000
WIN 8.1.	12000	2	24000
WIN EMB PosReady 2009	8000	5	40000
Итого, рублей. НДС не облагается:			263 000,0
Серверное оборудование и офисные ПК			
Сервер расчетный Intel Xeon	125000	1	125000
Сервер продажный Intel Xeon	125000	1	125000
Шкаф серверный 19" 22U	25000	1	25000
Полка к шкафу 19"	2300	2	4600
Блок розеток 19"	2700	2	5400
Патч-панель 19"	3000	2	6000
ИБП 1500	30000	1	30000
POS-компьютер моноблок Sam4s SPT-4700	60000	5	300000
Принтер SAM4S ELLIX 50DB	13000	5	65000
ШТРИХ-М-ФР-К	31500	1	31500
Итого, рублей в т.ч. НДС 18%:			717 500,0
Услуги			
Монтажные, пусконаладочные работы	30000	1	30000
Настройка рабочих мест	6000	7	42000
Настройка серверов	10000	2	20000
Транспортные/накладные расходы		1	21525
Итого, рублей в т.ч. НДС 18%:			113 525,0

Рисунок 5.1 - Коммерческое предложение от системы Tillypad.

2. Iiko

iiko (айко) — самая современная и мощная система на рынке автоматизации предприятий общественного питания. На базе iiko Вы сможете автоматизировать как маленькое кафе или большой ресторан, так и целую сеть заведений.

С помощью системы iiko вы сможете автоматизировать склад и продажи в ресторане, постоянно контролировать персонал (премировать в случае хороших продаж, автоматически штрафовать в случае нарушений). Сможете привлекать в ресторан, уже улучшенный при помощи этой системы автоматизации, новых посетителей, благодаря системе лояльности. Получите возможность управлять резервами, банкетами и дисконтными картами.

С Айко вы сможете быстро и точно проводить инвентаризацию, как на складе, так и на баре, ввести депозитную систему и даже учет доставок. Благодаря обширному блоку отчетности вы сможете всегда получить актуальный отчет о прибылях и убытках, проинспектировать управленческий баланс. С помощью системы событийного видео наблюдения вы сможете верно разобраться в возникших конфликтных ситуациях и наказать виновных.

Главные преимущества iiko (айко):

- быстрое и чёткое обслуживание ваших гостей благодаря удобному внесению и обработке заказов;
- прозрачное и быстрое построение управленческой отчетности для владельцев бизнеса;
- возможность контроля ключевых показателей заведения с мобильного телефона;
- кассовая книга, план счетов МСФО;

- обширная аналитика для маркетинга;
- решение для автоматизации прекрасно приспособлена для управления ресторанными сетями.

И с точки зрения защиты:

- работа кассовых станций в автономном режиме при обрыве локальной сети в iiko;
- возможность использования резервных принтеров ресторана;
- большие возможности настройки правами доступа;
- система автоматизации оповещения о внештатных ситуациях;
- автоматическое резервное копирование базы данных.

№	Номенклатура	Кол-во	Ед.	Цена	Сумма без скидки	Скидка	Сумма
Программное обеспечение							
1	iko Server сервер iko в ресторане	1	шт	23 990,00	23 990,00	1 199,50	22 790,50
2	ikoOffice автоматизация управления складом, персоналом, финансами (лицензия для одного АРМ бэк-офиса)	1	шт	11 990,00	11 990,00	599,50	11 390,50
3	ikoFront автоматизация кассовой станции(лицензия для одного АРМ фронт-офиса)	9	шт	19 990,00	179 910,00	8 995,50	170 914,50
4	ikoTableService автоматизация ресторанов с официантским обслуживанием (лиц. для 1 АРМ)	9	шт	9 990,00	89 910,00	4 495,50	85 414,50
	Итого по: Программное обеспечение				305 800,00	15 290,00	290 510,00
Оборудование							
5	Сенсорный моноблок AnyShop D 25	9	шт	41 000,00	369 000,00		369 000,00
6	Чековый принтер SPARK-PP- 2010.2A (сетевой)	13	шт	9 200,00	119 600,00		119 600,00
7	Фискальный регистратор ККМ ШТРИХ-М-ФР-К RS/USB	1	шт	29 500,00	29 500,00		29 500,00
8	Денежный ящик Штрих CD	1	шт	2 700,00	2 700,00		2 700,00
	Итого по: Оборудование				520 800,00		520 800,00
Работы							
9	Автоматизация: Установка и настройка рабочего места	10	шт	6 000,00	60 000,00	12 000,00	48 000,00
10	Автоматизация: Обучение персонала БЭК-офиса	1	шт	12 000,00	12 000,00	2 400,00	9 600,00
11	Автоматизация: Обучение персонала Фронт-офиса	1	шт	4 000,00	4 000,00	800,00	3 200,00
12	Абонентское обслуживание ресторанов (ЛИТС: Standart) (3 месяца)	1	шт	14 850,00	14 850,00		14 850,00
13	База iko сервер в облаке (1 месяц)	1	шт	3 300,00	3 300,00		3 300,00
	Итого по: Работы				94 150,00	15 200,00	78 950,00
Итого:					920 750,00	30 490,00	890 260,00

Рисунок 5.2 – Коммерческое предложение от системы Iiko.

3. R-Keeper

Программный комплекс R-Keeper™ - профессиональная система автоматизации для предприятий общественного питания: ресторанов, кафе, баров и других заведений, как одиночных так и сетевых.

С R-Keeper™ ресторатору доступны все необходимые инструменты управления рестораном, складом и производством, а также инновационные

технологические решения по организации эффективной работы персонала ресторана и управлению лояльностью гостей: мобильные терминалы официанта на базе Apple iPod Touch, виртуальная карта гостя, электронное меню на планшете iPad, кассовые станции с дополнительным экраном для гостя, интеллектуальная система событийного видеоконтроля за кассовой зоной, система автоматического резервирования столов, CRM-система, система удаленного мониторинга работы ресторана, система автоматизации службы доставки, система автоматизации склада и другие.

Полная автоматизация предприятия общепита обеспечивается двумя программными уровнями: кассовым и менеджерским. Кассовый (оперативный) уровень обеспечивает автоматизацию процесса продаж и формирование базы данных по продажам. Менеджерский уровень (офис ресторана) отвечает за формирование справочников, распределение прав доступа, разнообразные настройки кассового уровня, установку параметров и настроек отчетов, разработку и внедрение маркетинговых программ, обеспечение необходимого взаимодействия с другими системами.

Для автоматизации складского учета в системе R-Keeper используется программа [StoreHouse](#), позволяющая полностью контролировать процесс управления производством в ресторанах, кафе и ресторанах быстрого обслуживания. Совместимость StoreHouse с системой бухгалтерского учета 1С:Бухгалтерия позволяет пользователю на основе документов StoreHouse автоматически формировать в 1С:Бухгалтерия журнал операций и журнал проводок. Специализированный OLE-сервер обеспечивает 1С:Бухгалтерия непосредственный доступ к данным StoreHouse, что упрощает взаимодействие этих двух программ.

Система R-Keeper работает на различных кассовых аппаратах и официантских терминалах (станциях), которые объединены в локальную сеть. Станции по

своему назначению и функциональным возможностям разделяются на четыре вида:

- станция кассира;
- станция официанта;
- станция бармена;
- компьютер менеджера.

Коммерческое предложение

Таблица 2.1 – Коммерческое предложение от системы R-Keeper.

Наименование	Цена (руб)	Кол-во	Сумма	Комментарии
Кассовое оборудование				
ККМ RR-Electro RR-02K	32 000,00	1	32 000,00	Фискальный регистратор с возможностью печати двухмерных кодов для регистрации продаж алкоголя в ЕГАИС. Высокий ресурс авторезчика, термолента 80мм.
Денежный ящик	3 600,00	1	3 600,00	Денежный ящик. Программируемые режимы открытия (при оплате наличными, по запросу менеджера и т.п.)
Итого кассовое оборудование			35 600,00	

Станции

Моноблок ECOPOS 15", Windows POSReady	64 000,00	8	512 000,00	Моноблок, Touch Screen 15", HDD, MCR, 2Gb RAM, LAN, Windows POSReady 2009. 3 года гарантия. Станция кассира\официанта профессионального уровня. Программные настройки R- Keeper 7 возможно быстро производить удаленно, не прибегая к вызову инженера.
Пластиковая магнитная карта	60,00	100	6 000,00	Пластиковая магнитная карта для авторизации персонала.
Итого станции			518 000,00	

Принтеры

Принтер Sam4s Ellix 50	12 500,00	13	162 500,00	USB\COM\Ethernet
Патч-корд	150,00	13	1 950,00	
Итого принтеры			164 450,00	

Компьютерное оборудование

Сервер баз данных	55 500,00	1	55 500,00	Сервер с зеркальным массивом для защиты данных. MidTower
Итого компьютерное			55 500,00	

оборудование**Программное****обеспечение****R-Keeper V7**

Касса - R-Keeper	24 000,00	1	24 000,00	Программный модуль для ст.кассира. Функционал официанта, проведение оплат и работа с фискальным регистратором (снятие отчетов, инкассация, закрытие смены и т.д.)
Официант - R-Keeper	18 000,00	8	144 000,00	Программный модуль для ст.официанта
Менеджер - R-Keeper	30 000,00	1	30 000,00	Программный модуль для ст.менеджера. Гибкие настройки ресторана. Редактирование справочников, управление правами персонала. Настройка функционала и расположения форм в модулях кассира и официанта. Детальные предустановленные отчеты, а так же конструктор отчетов на основе OLAP - технологии.

Склад - Store House	42 000,00	1	42 000,00	Программный модуль складского учета. Работа с технологическими картами, инвентаризации, контроль остатков, алкогольная декларация с сертифицированной поддержкой ЕГАИС, OLAP конструктор отчетов и другой функционал. Полный контроль над процессом производства в ресторане.
Итого программное обеспечение			240 000,00	

Услуги

Пуско-наладочные работы	6 000,00	12	72 000,00	Монтаж оборудования, инсталляция ПО
Проектное сопровождение	25 000,00	1	25 000,00	Предпроектное обследование, технические консультации, оптимизация процесса внедрения под конкретного заказчика, формирование структурных схем, схем печати
Обучение по программе R-Keeper Cashier	6 000,00	1	6 000,00	4 часа. Официант, кассир, администратор

Обучение по программе R-Keeper v7 Manager	9 000,00	1	9 000,00	6 часов. Администратор
Обучение по программе Store House	21 000,00	1	21 000,00	14 часов. Бухгалтер, калькулятор
Итого услуги			133 000,00	
Итого по данному договору: 1 091 050,00				

Таблица 3 – Сравнение выбранных систем.

Функция/Процесс	1С решения	iiko	R-Keeper	TillyPad XL
Финансовый и управленческий функционал				
Управленческий план счет(настраиваемый), двойная запись	нет	да	нет	нет
Отчет о прибылях и убытках	нет	да	нет	нет
Баланс предприятия	нет	да	нет	нет
Отчет о движении денежных средств	да	да	да	да
Ведение бюджета по статьям, план/факт анализ	да	да	нет	да
Учет продаж				
Шведский стол	да	да	нет	нет
Резервирование столиков	нет	да	да	нет
Учет питания сотрудников	да	да	нет	да
Модуль управления билльярдом	нет	да	да	нет
Модуль управления доставкой	нет	да	нет	да
Дозатор розлива напитков	нет	нет	да	да
Рабочий терминал шеф-повара	нет	да	нет	нет
Учет товаров				
Инвентаризация на баре с использованием весов и сканера ШК	нет	да	нет	нет
Работа с отрицательными остатками на складе	нет	да	нет	да
Пересчет остатков задним числом по факту изменения тех. карт	нет	да	нет	да
Контроль допустимых остатков	нет	да	да	нет
Контроль закупочных цен	нет	да	нет	нет
Раскрутка полуфабрикатов и блюд на остатках	нет	да	нет	да
Формирование стоп-листа	нет	да	нет	нет
Формирование заказов под банкеты	нет	да	нет	нет
Управление персоналом				
Автоматический расчет сдельной ЗП (включая налоги)	нет	да	нет	нет
Автоматическое начисление штрафов за нарушение трудовой дисциплины	нет	да	нет	нет
Ведение графика выходов персонала на работу	нет	да	нет	нет
Личный отчет по ЗП	нет	да	нет	нет
Производство блюд и полуфабрикатов				
Составление блюд и калькуляций	да	да	да	да
Работа с вложенными блюдами	да	да	да	да
История изменения тех. карт	да	да	да	да
Управление лояльностью				
Дисконтные системы	да	да	да	да
Бонусные системы	нет	да	да	нет
Привлечение новых клиентов	нет	iiko.NET	нет	нет
Бухгалтерский и налоговый учет				
Обмен данными с бухгалтерией	да	да	да	да
Автоматическое формирование алкодекларации	нет	да	да(версия 7)	нет
Ведение бухгалтерского учета	да	нет	нет	нет

В таблице 3 по мимо сравниваемых трех системы, приведена еще для общего сравнения, система 1с.

В конечном итоге, из расчета коммерческого предложения и функционала выбор пал на программное обеспечение iiko.

Перечислим еще раз основные отличия программы для автоматизации ресторанов iiko от конкурентных решений:

- Система автоматизации ресторанов позволяет получать данные по текущей выручке, среднему чеку, количеству гостей, себестоимости, среднему времени обслуживания гостя и многим другим показателям в реальном времени на экране мобильного телефона IOS, что дает возможность оперативно принимать верные управленческие решения;
- Система позволяет осуществлять визуализацию информации в виде графиков для любых показателей, добавлять любое количество показателей и изменять их расположение произвольным образом, для упрощения восприятия отчетной информации;
- Наблюдение за сотрудниками, регулировку работы кухни и ознакомление с отчетами можно выполнять из любой точки планеты, где есть доступ к всемирной сети.

3 Проектная часть
3.1 Проектирование wi-fi сети.

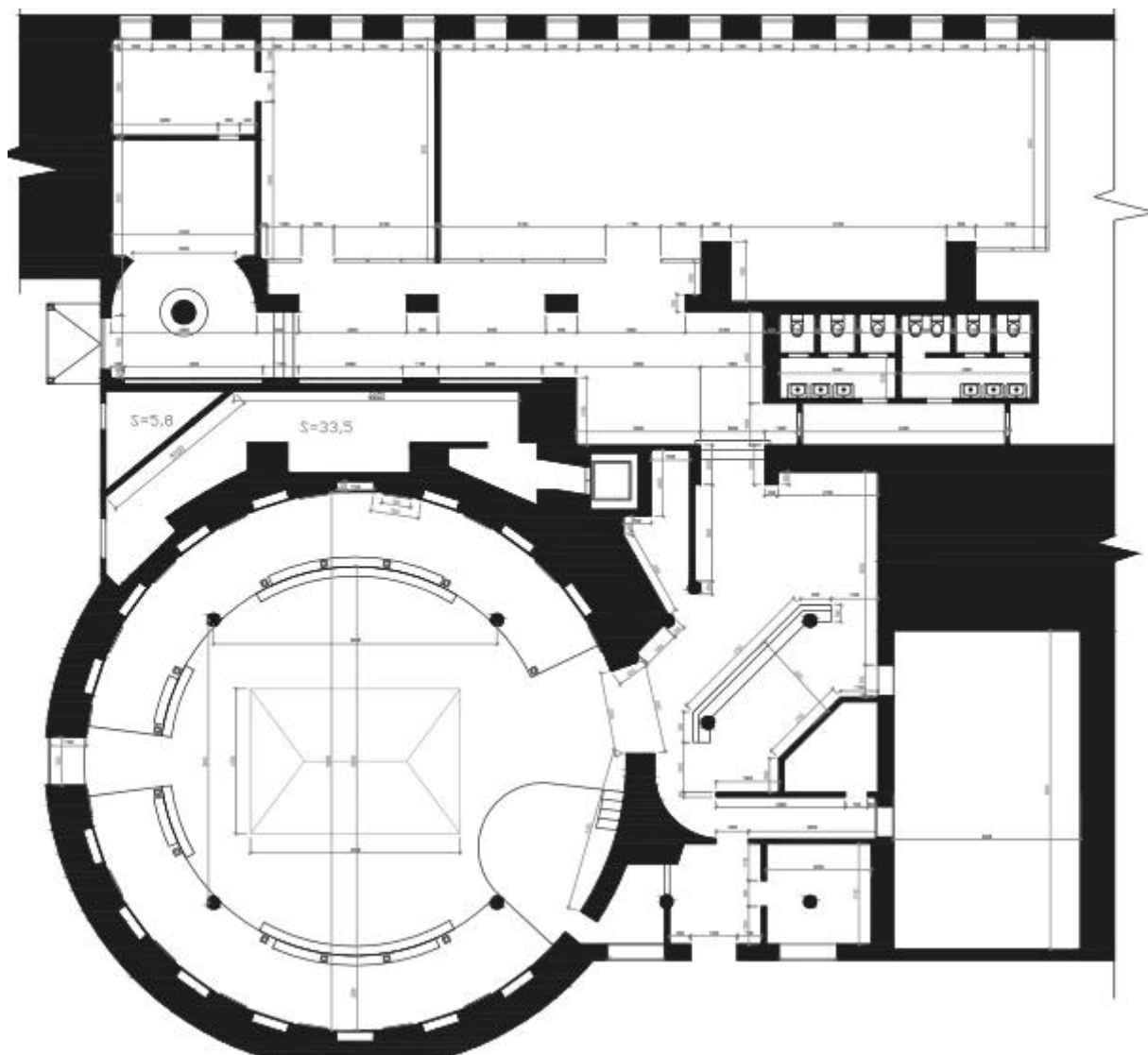


Рисунок 6.1 – Схема ресторана.

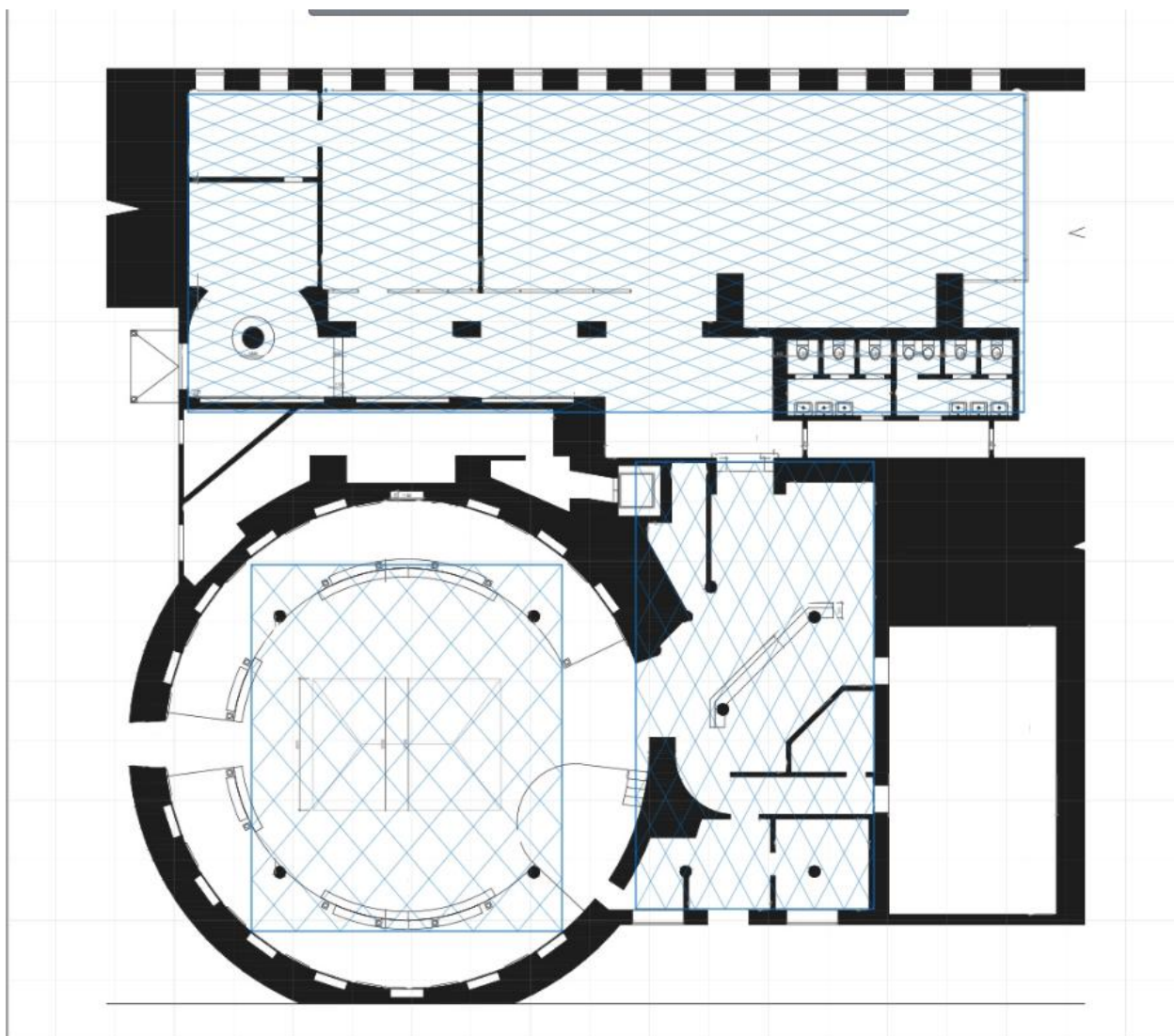


Рисунок 6.2 – Нанесение на схему зон покрытия wi-fi.

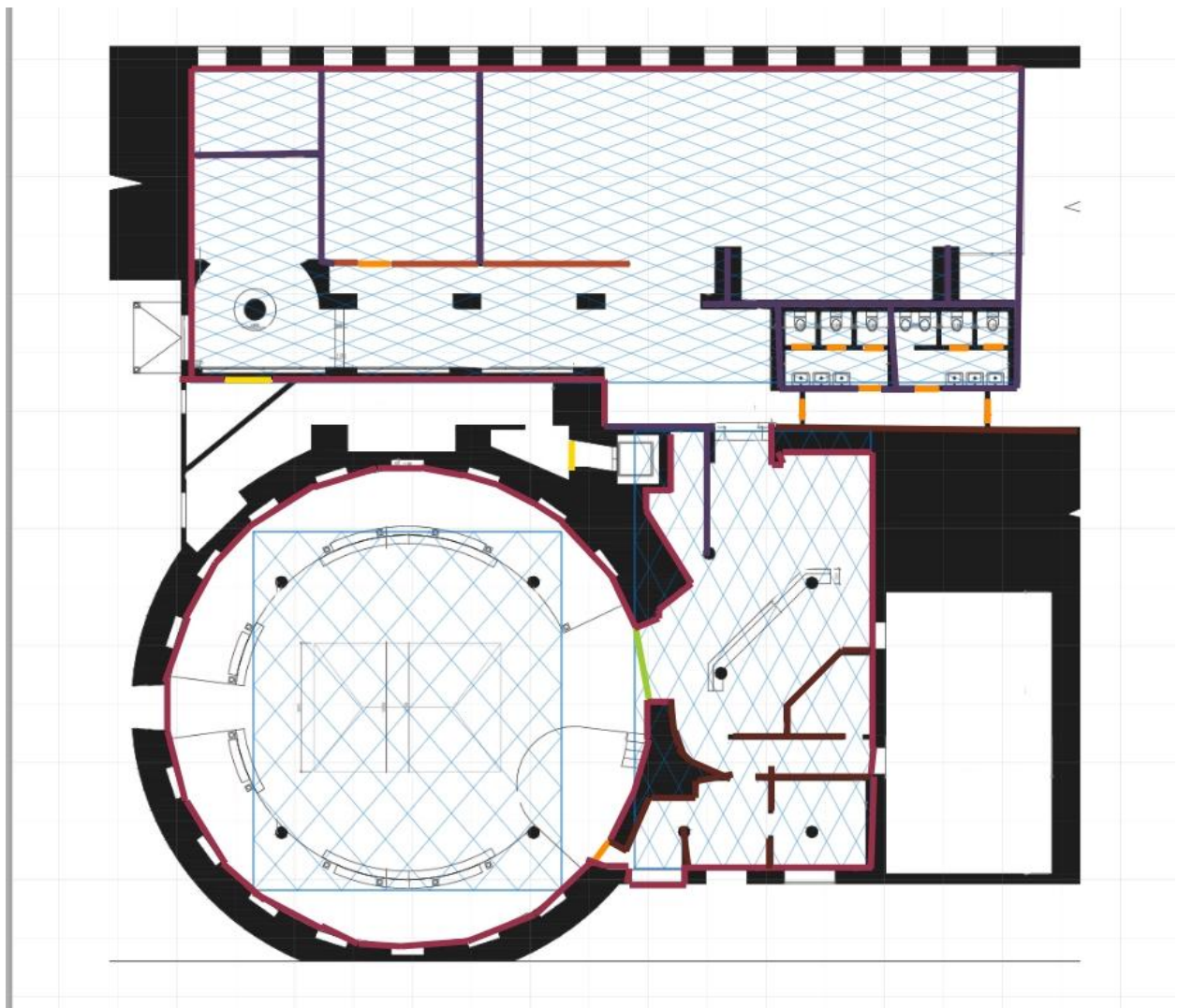


Рисунок 6.3 – Нанесения на схема текстуру стен, дверей, окон.

 Dry Wall (4 dB)	 Wood Wall (4 dB)
 Plastic Wall (4 dB)	 Glass Wall (8 dB)
 Brick Wall (8 dB)	 Concrete Wall (12 dB)
 Light Door (4 dB)	 Metal Door (11 dB)
 Heavy Door (15 dB)	
 Thin Window (2 dB)	 Thick Window (4 dB)

Рисунок 6.4 – Соответствие цвета с материалом.

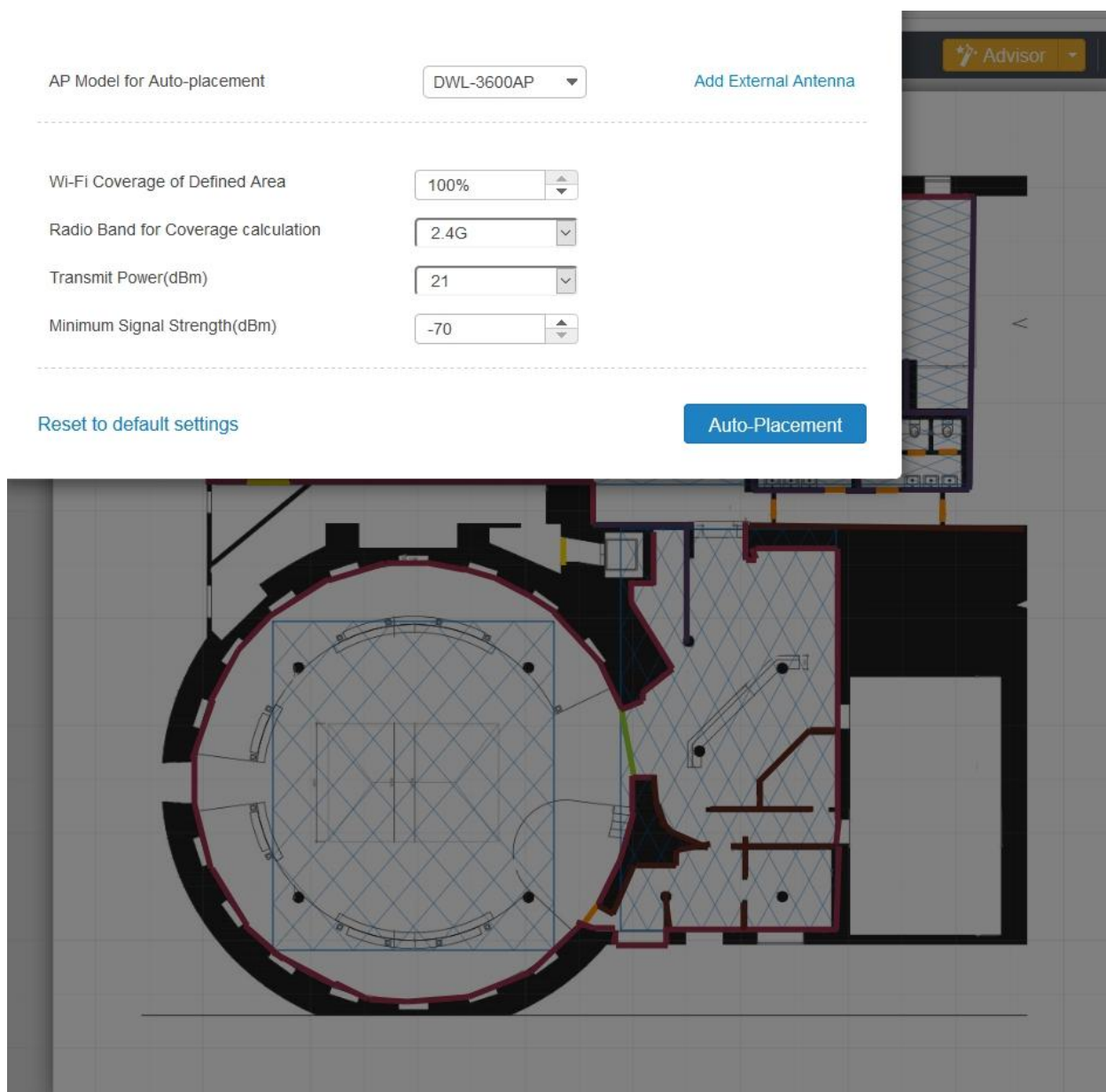


Рисунок 6.5 – Выбор точки доступа.

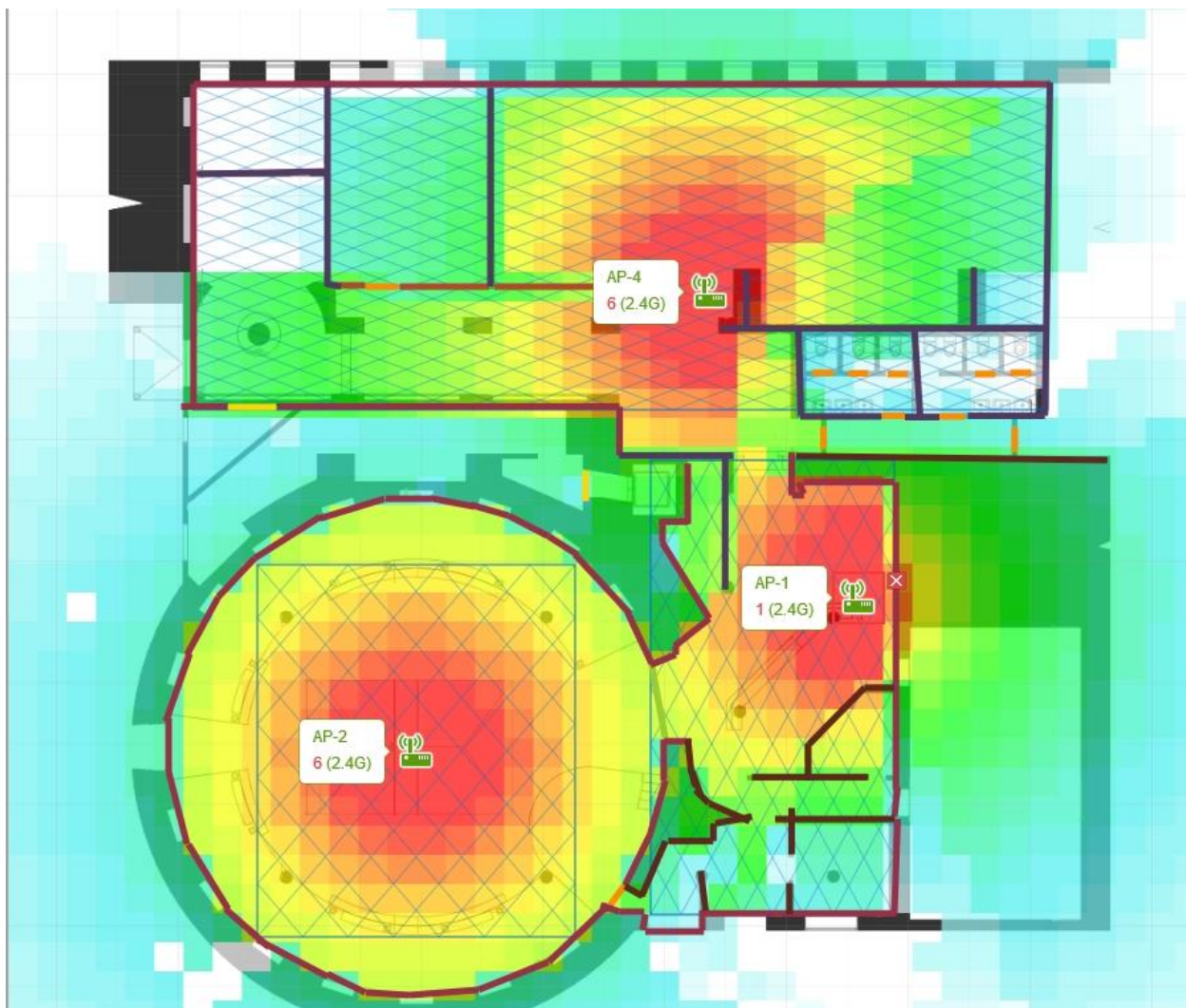


Рисунок 6.6 – Покрытие зон сетью Wi-Fi

На рисунке 6.1 представлена план схема ресторана.

На рисунке 6.2, обозначены зоны, в которых по проекту, должен быть максимально высокий уровень приема сети wi fi. В виду того, что пропускная способность сети wi fi зависит от окружающих предметов, и материала стен, на рисунке 6.3 показано нанесение на план схему видов стен и дверей. Материал стен и виды дверей относительно их цвета на плане показаны на рисунке 6.4.

После всех манипуляций с план схемой, выбираем наше оборудование. Рисунок 6.5. После всех вычислений, на план схеме сформированы идеальные места установки для wi fi точек. Рисунок 6.6 Здесь же мы видим на каком канале выгоднее всего будет работать наше оборудование. Точка AP-1 на первом канале и точки AP-4 и AP-2 на втором.

3.2 Проверка расчетов программы

При выборе модели распространения сигнала руководствовались планом помещения, его особенностями построения.

Статистическая модель, рекомендованная Международным институтом электросвязи ITU-R 1238, была разработана для расчета распространения сигнала внутри зданий и помещений.

Данная модель учитывает потери при многократном прохождении сигнала через пол, что позволяет предусмотреть такие характеристики, как повторное использование частоты на различных этажах здания.

Дистанционные коэффициенты потери мощности, включают в неявном виде поправку на потери при прохождении сигнала через стены или через препятствия, а также на остальные механизмы возникновения потерь, которые могут возникнуть в пределах одного этажа здания. Данная модель показана в виде формулы 1:

$$L = 20 \log f + N \log d + P_f(n) - 28 \quad (1)$$

где, d – расстояние в метрах;

f – частота в мегагерцах;

N – коэффициент потери мощности сигнала с расстоянием;

n – количество препятствий;

$P_f(n)$ – параметр потери мощности сигнала при прохождении через препятствия.

Характерные параметры, основанные на результатах различных измерений, приведены в справочных данных, в данном случае значения берем для офисных помещений, а именно для $N=30$ для частоты 2.4ГГц и параметр потери мощности $P_f(n)=14$ [2].

Расчеты, приведенные для неперекрывающихся каналов 1 (2412 МГц), 6 (2437 МГц), 11 (2462 МГц) для радиуса покрытия 15 метров:

$$L_{ch1} = 20 * \log(2412) + 30 * \log(8) + 14 - 28 = 80.74 \text{ дБ}$$

$$L_{ch6} = 20 * \log(2437) + 30 * \log(8) + 14 - 28 = 80.83 \text{ дБ}$$

$$L_{ch11} = 20 * \log(2462) + 30 * \log(8) + 14 - 28 = 80.92 \text{ дБ}$$

Расчет работоспособности тракта передачи для выбранной внутренней точки доступа DWL-3600AP, данные для расчета берутся из технических характеристик точки доступа, указанных выше в пункте 1.4 таблица 3.

$$20 - (-68) = 88 \text{ дБ}$$

3.3 Определение количества точек доступа для выбранного помещения

Существует два способа определения количества точек доступа при проектировании сети беспроводной передачи данных для помещений. Первый способ рассматривает покрытие помещения зонами в форме квадрата, а второй способ в форме шестигранника. Наглядное использование данных способов приведено на рисунках 3.1 и 3.2.

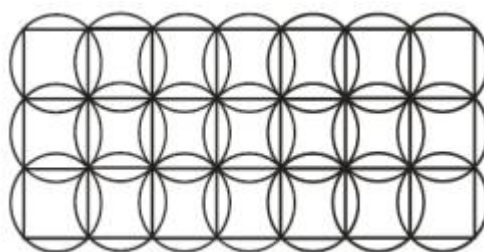


Рисунок 3.1 – Покрытие зон в форме квадратов.

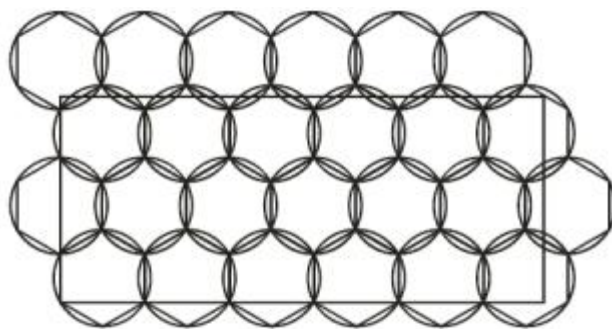


Рисунок 3.2 – Покрытие зон в форме шестигранника.

Так как выбранное помещение имеет большую площадь и простую планировку, то для простоты расчетов выбираем первый способ определения количества точек доступа. Расчет производится по формуле 2.

$$S = \left(\frac{a}{(r - t) * \sqrt{2}} \right) * \left(\frac{b}{(r - t) * \sqrt{2}} \right)$$

где a – длина помещения;

b – ширина помещения;

r – радиус покрытия одной точки доступа;

t – необходимое пересечение зон.

Для данного помещения производим расчет количества точек:

$$S = \left(\frac{32}{(15 - 2) * \sqrt{2}} \right) * \left(\frac{30}{(15 - 2) * \sqrt{2}} \right) = 2.88$$

Данное значение округляем в большую сторону, следовательно, для покрытия помещения необходимо 4 точки доступа. [3]

Для наглядности на рисунке 7 приводится схема соединений оборудования.

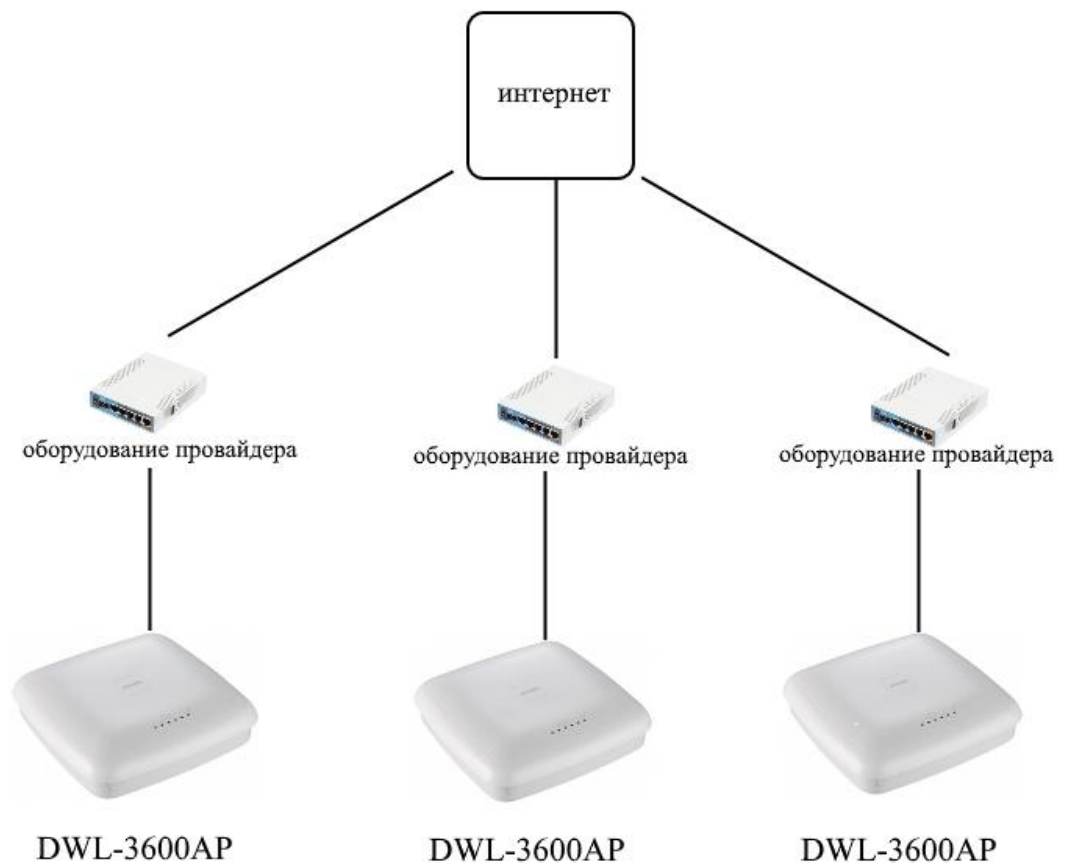


Рисунок 7 – Структурная схема оборудования.

3.4 Проектирование видеонаблюдения и рабочей сети

Аппаратное обеспечение видеонаблюдения это электронные и механические части вычислительного устройства, входящие в состав системы или сети, исключая программное обеспечение и данные (информацию, которую вычислительная система хранит и обрабатывает). Аппаратное обеспечение включает: компьютеры и логические устройства, внешние устройства и диагностическую аппаратуру, энергетическое оборудование, батареи и аккумуляторы.

Рассмотрим тип систем видеонаблюдения - специализированный комплект оборудования (СК). Необходимо отметить, что относительно дешевые системы видеонаблюдения специализированного комплекта во всех

отношениях хуже аналогичных на базе типового компьютера. Системы на базе специализированного комплекта являются дорогими. Приобрести такую систему и содержать – достаточно затратная статья расходов для предприятия [21]. Системы видеонаблюдения (СК) обладают следующими достоинствами:

- специализация и компактность;
- развитые функции охранной и пожарной сигнализаций, контроль доступа;
- одновременное обслуживание десятков камер слежения;
- соответствие специальным требованиям по безопасности, сертификат соответствия.

Система видеонаблюдения (СК) включает обязательные компоненты:

- видеокамеры;
- видеомониторы;
- квадраторы (если используется четыре видеокамеры)
- видеомультиплексоры (если используется от 4-х до 32-х видеокамер);
- матричные коммутаторы видеосигнала (если число камер более 32)
- специальные видеомagneтофоны длительной записи;
- видеомониторы специализированного комплекта (не на базе компьютера).

Видеомонитор - это устройство отображения картинки, передаваемой видеокамерой или сохраненной в архиве.

При выборе видеомонитора учитывается ряд характеристик.

Размер экрана - для охранного видеонаблюдения применяются видеомониторы с размером экрана от 5 до 21" (дюйма) по диагонали (один дюйм равен 2,54 см); - разрешение (количество горизонтальных строк, отображаемых видеомонитором). Измеряется в ТВ-линиях. В зависимости от типа монитора этот параметр может составлять от 300 до 1000 ТВ-линий.

Количество видеовходов (число подключенных источников видеоизображения, например, видеокамер) -как правило, видеомониторы содержат один, два или четыре видеовхода, переключение между которыми может производиться в ручном или автоматическом режиме (через заданное время).

Наличие сервисных функций (встроенный квадратор, аудиоканал, "тревожные" входы и т.д.).

Недостатки системы видеонаблюдения специализированного комплекта (СК):

- видеозапись во многих системах СК ведется на магнитофонную ленту. Поэтому поиск нужного видеофрагмента в таких системах крайне затруднен;
- кассеты с лентой, на которой записана видеоинформация, уязвимы для размагничивания;
- ремонт оборудования систем видеонаблюдения возможен только в специализированных мастерских [21].

В последнее время произошло некоторое затоваривание продукции систем видеонаблюдения СК. Причина с одной стороны та, что очень быстро совершенствуются системы на базе КК - мощная конкуренция. С другой стороны, в комплект подавляющего большинства систем СК входят устаревшие мониторы с электронно-лучевыми трубками, выделяющие много тепла, потребляющие много электроэнергии, излучающие при работе вредные для здоровья тяжелые ионы. Причем, заменить такой монитор на компьютерный жидкокристаллический, невозможно.

Рассмотрим второй тип систем видеонаблюдения - компьютерная система видеонаблюдения (КК). Система видеонаблюдения на базе типового компьютера включает следующие компоненты: компьютер; плата системы видеонаблюдения (плата видеозахвата); программное сопровождения платы видеонаблюдения; видеокамеры. Недостатком видеосистем КК является

невозможность одновременного обслуживания (напрямую, без платы расширения) свыше восьми камер слежения [22].

Еще один недостаток системы видеонаблюдения КК является сложность приемлемого выбора из огромного количества вариантов и производителей. Для видеоконтроля в небольших офисах и на складах, для наружного и внутреннего видеонаблюдения в квартирах и на дачах бывает вполне достаточно установки от одной до восьми камер слежения, сигналы от которых способен обработать любой современный компьютер. Даже если для видеонаблюдения требуется больше восьми видеокамер, то как вариант можно применить второй точно такой же комплект системы видеонаблюдения на базе компьютера. Стоимость двух компьютерных комплектов все равно окажется гораздо дешевле одной аналогичной системы на базе специализированного комплекта.

Исходя из проведенного анализа оптимальный выбор - система видеонаблюдения на базе компьютера (КК).

Минимальный состав основного комплекта для оборудования системы видеонаблюдения - типовой компьютерный комплект (системный блок, монитор, бесперебойное питание, модем); - плата видеозахвата системы видеонаблюдения (адаптер системы видеонаблюдения КК); - комплект программного обеспечения системы видеонаблюдения (к плате видеозахвата); - видеокамеры видеонаблюдения - источник (адаптер) питания 220/12 вольт на ток 1 или 2 ампера - кабельная разводка от адаптера питания к видеокамерам и от видеокамер к компьютеру

Требования к плате системы видеонаблюдения: - работа с программным обеспечением, совместимым с операционной системой Windows XP / Vista / 7; - аппаратно в реальном времени кодирование видеосигнала от камер слежения в архивный информационный формат . Круглосуточно работающая система видеонаблюдения даже в самом медленном режиме от нескольких камер обрабатывает очень много видеoinформации. При необходимости (или в плановом порядке) ее просмотр и поиск нужного фрагмента может занимать

очень много сил и времени.

Видеозапись в этом случае осуществляется только в то время, когда на этом участке объекта (экрана) есть движение. Как уже говорилось, система видеонаблюдения состоит из камер слежения и средств записи - отображения видеоинформации. Задача видеокамер охватить как можно более подробно контролируемое пространство [21].

Иногда для расширения зоны обзора применяют поворотные устройства видеокамер, при этом следует учесть что:

- стоимость поворотного устройства в несколько раз больше, чем стоимость видеокамеры;
- при повороте изменяется фокусное расстояние до объекта, поэтому приходится применять дорогие камеры с функцией регулировки фокусного расстояния;
- поворотное устройство имеет ограниченный температурный диапазон, в то время для видеокамеры в термокожухе такого ограничения не существует;
- управление поворотным устройством требует дополнительной проводки и специального программного сопровождения;
- механизм поворота потребляет дополнительную электроэнергию;
- важное событие может произойти именно в том секторе, от которого только что "отвернулась" камера;
- программный "детектор движения" системы не работает с двигающейся камерой;
- сложный механизм устройства поворота снижает надежность всего узла в целом .

С учетом вышесказанного, для расширения зоны видеонаблюдения целесообразней увеличивать число видеокамер, а поворотные устройства применять лишь в исключительных случаях.

Платы видеонаблюдения характеризуются:

- количеством каналов (максимальное число камер слежения), обрабатываемых одной платой;

- наличием и количеством аудио (звуковых) входов; - возможностью аппаратного кодирования видеосигнала в стандартные видеоформаты;

- развитостью функциональных возможностей программного обеспечения. Компьютерная система видеонаблюдения включает следующие компоненты:

- компьютер;
- плата системы видеонаблюдения;
- программное сопровождения платы видеонаблюдения;
- видеокамеры;
- матричные коммутаторы видеосигнала (если число видеокамер превышает8).

Проведя анализ аппаратного обеспечения, пришли к выводу, что для ресторана «Квартира Кости Кройца» наиболее оптимально будет использование системы видеонаблюдения на базе компьютера (КК).

Минимальные требования к конфигурации ПК:

- процессор: Pentium 4 2.8 ГГц (или аналог AMD);
- оперативная память: 2 Гб;
- жесткий диск: 60 Гб;
- звуковая карта: необходима при использовании микрофона (обратной связи) или звуковой сигнализации;
- видеокарта: не ниже NvidiaGeforce FX5200 или ATI RADEON 7000 (9000), 256 Мб ОЗУ.

Программное обеспечение:

- Microsoft.NET Framework 2.0 или выше;
- DirectX 9.0сот августа 2009 года или выше;

– Кодеки для воспроизведения MPEG-4 (рекомендуется K-ite 470F или более новые).

Необходимо учитывать особенности, которые в итоге влияют на отказоустойчивость и надежность системы. Некоторые продукты позволяют добавить видеонаблюдение к системе безопасности, иные – выступают в качестве ядра, с которым интегрируются другие системы, расширяющие и дополняющие базовый функционал.

При создании комплексных систем безопасности, включающих в себя кроме систем видеонаблюдения также и системы контроля и управления доступом возможно интеграция обеих систем в единое целое, причем в зависимости от степени интеграции конкретной системы в конкретное программное обеспечение интеграция происходит либо на уровне контроллеров (они подключаются к серверу видеонаблюдения) либо на уровне серверов (сервер СКУД подключается к системе видеонаблюдения).

Выбор программного обеспечения в данном случае в первую очередь зависит от выбранной СКУД и ее поддержки системой видеонаблюдения. Как правило, программные модули интеграции со СКУД лицензируются и приобретаются дополнительно[22].

Далее рассмотрим программное обеспечение для построения системы видеонаблюдения. При обзоре программ (прил. 4) для построения системы видеонаблюдения выбор был сделан в пользу программного обеспечения «Линия» (www.devine.ru), так как ПО «Линия» обладает широкими функциональными возможностями и приемлемой стоимостью.

Система видеонаблюдения «Линия», разработанная российской компанией «ДевЛайн». Торговая марка «Линия» включает в себя три варианта поставки: видеосерверы с одноименным названием, платы видеозахвата «Линия Hybrid IP», софт «Линия IP», предназначенный только для работы с IP-камерами.

Программное обеспечение «Линия» поставляется со всеми продуктами компании, не имеет сетевых, административных и функциональных

ограничений.

Программное обеспечение системы «Линия» состоит из двух частей — оболочки и ядра. Ядро системы предназначено для захвата и обработки видео и аудиоданных согласно пользовательским настройкам и работает незаметно для пользователя. Запускается ядро автоматически перед авторизацией Windows и работает, записывая данные и передавая их при необходимости в сеть, даже если оболочка закрыта.

Оболочка ПО «Линия» предназначена для взаимодействия с ядром системы, осуществления пользовательских настроек и просмотра видео и аудиоданных. Оболочка состоит из трех разделов.

«Наблюдательный пост» - предназначен для просмотра изображения с видеокамер и прослушивания звука в режиме реального времени. Наблюдение может осуществляться как на локальном, так и на удаленном компьютере. Интерфейс системы видеонаблюдения «Линия» представлен на рис.8.

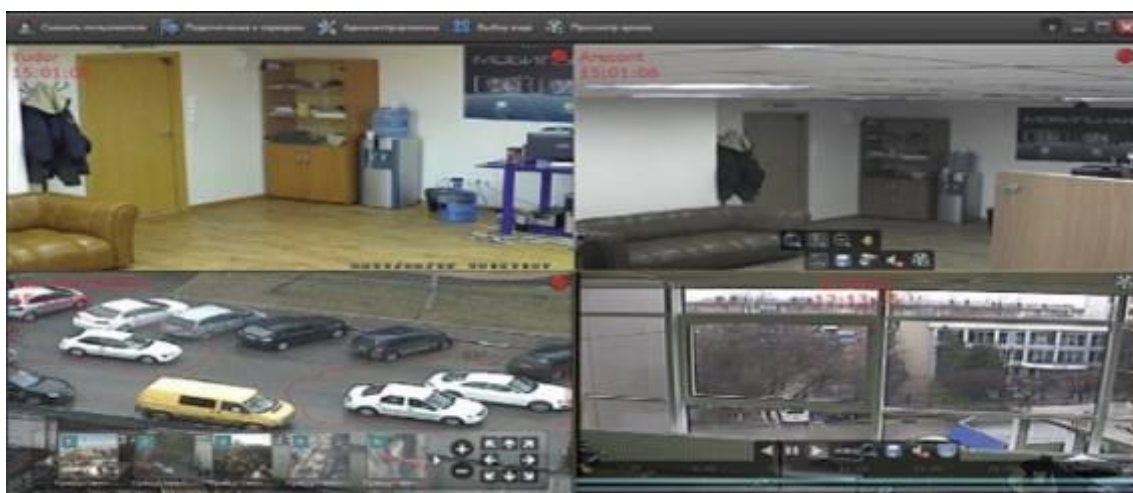


Рис. 8 Интерфейс системы видеонаблюдения «Линия»

«Администрирование» — часть оболочки, предназначенная для настройки работы всей системы «Линия».

«Просмотр архива» — предназначен для просмотра архива и экспорта в удобный формат уже записанной информации.

ПО «Линия» позволяет объединять в одном сервере как аналоговые, так

и IP-видеокамеры, совмещая преимущества первых и вторых.

Охранное видеонаблюдение будет работать круглосуточно.

В случае перебоев с электроэнергией система охранного видеонаблюдения переходит на работу от резервируемого источника питания (ИБП) и работает время, в течение которого обслуживающий персонал отреагирует на аварию и примет соответствующие меры.

Сервер видеонаблюдения и центральный коммутатор требуется расположить в кабинете охраны. Сервер, ведёт контроль за работой видеокамер и обрабатывает поступающую видеоинформацию.

Подключаться камеры будут посредством технологии PoE.

PoE или PoweroverEthernet - технология позволяющая передавать удалённому устройству вместе с данными электрическую энергию через стандартную витую пару в сети Ethernet. PoweroverEthernet стандартизирована по стандарту IEEE 802.3af-2003. Согласно данному стандарту обеспечивается постоянный ток с номинальным напряжением 48 В. через две пары проводников в четырёхпарном кабеле, с максимальным током 400 мА для обеспечения максимальной мощности 12,95 Вт [25].

Для подключения используется коммутатор. В данном случае будет присутствовать специальный сетевой коммутатор (маршрутизатор с большим количеством портов), к которому есть возможность подключить до 20-30 (а то и больше) камер видеонаблюдения. В данном случае 10 камер.

Применение коммутатора дает только выгоду - не требуются блоки питания для камер, нет необходимости прокладывать дополнительные провода для питания камер. Коммутатор имеет встроенную грозозащиту по питанию 220В и по Ethernet портам.

Коммутация всех устройств осуществляется при помощи «прямого» патч-корда, а настройка в соответствии руководством конкретного производителя (рис.9)



Рис. 9 – Схема подключения устройств.

В табл. 5 произведем расчет стоимости необходимого оборудования системы видеонаблюдения, на основе рассмотренных ранее характеристик камер видеонаблюдения.

Таблица 5 Расчёт стоимости оборудования системы видеонаблюдения

Категория оборудования	Производитель и модель	Цена, руб.	Количество, шт./м.	Стоимость, руб.
Персональный компьютер	DNS	20000	1	20000
IP-камера видеонаблюдения (внеш.)	Dlink DCS-4602ev	9300	2	18600
IP-камера видеонаблюдения (внутр.)	Dlink DCS-2230L	12000	8	96000
Коммутатор	Dlink DES-1210-28P	12400	1	12400
Кабель	UTP	5	305	1525

«Витая пара»				
Кабель-канал (короб)	ЕСО 40X16	26,73	80	2139
Коннектор	8P8C	2	20	40
ПО «Линия»	Линия А Hyb rid IP	16128	1	16128
Прочие расходные материалы	ЕСО	300	-	300
Итого				143532

Составим схему установки системы видеонаблюдения исходя из характеристик видеокамер и технического плана здания. Схема объекта видеонаблюдения представлена на рис. 10.

Для коммутации понадобится специальный кабель и разъемы. В качестве соединительного кабеля применяется «витая пара», а в качестве разъемов используются RG-45.

Для подключения всех устройств понадобится 100 м «витой пары».

Соединение разъема и кабеля осуществляется при помощи специального обжимного устройства, напоминающего пассатижи.

Когда кабель готов, видеокамеру необходимо соединить с сетевой картой компьютера и в соответствии с руководством пользователя назначить ей IP-адрес.

Для доступа к камере через Интернет набирают IP-адрес провайдера и добавленный к нему номер порта. Часто обязательным условием является статический адрес интернет провайдера. В противном случае он будет постоянно меняться и камеры будут недоступны. Если нет возможности использования статического адреса, то можно воспользоваться динамическим «белым» (т.е. с возможностью внешнего подключения) с привязкой адреса к

доменному имени или специальным сервисом видеонаблюдения провайдера.

Разработанная система видеонаблюдения позволяет: наблюдать за периметром ресторана; осуществлять видеозапись в формате AVI на жесткий диск персонального компьютера.

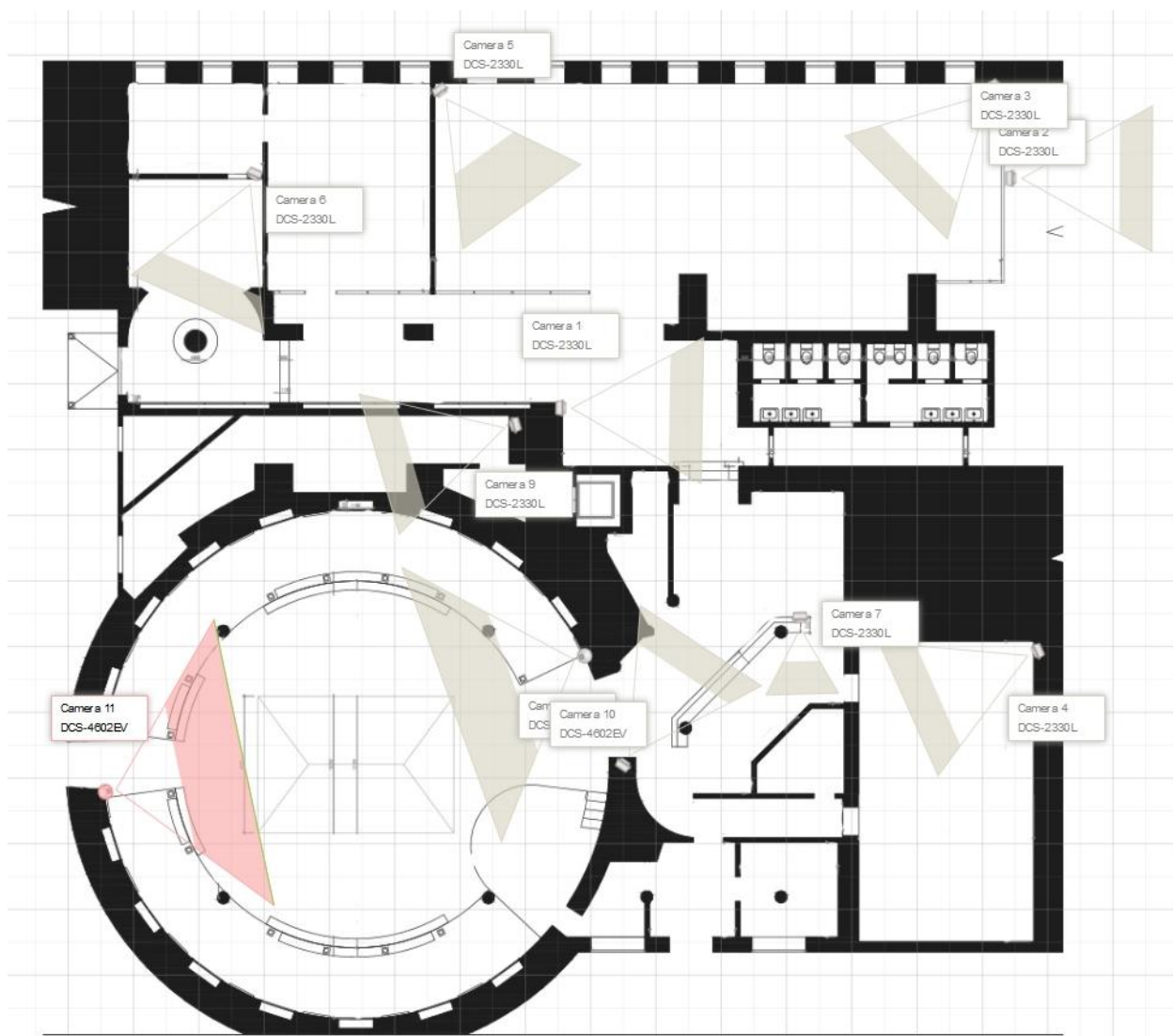


Рисунок 10 – Схема обзора камер.

3.5 Сеть

Для развертки офисной сети использовался роутер D-link DIR 320, с поднятым на нем NAT и DHCP. В свою очередь, этот роутер подключается к

коммутатору, использованному для системы видео наблюдения. По скольку в системе видео наблюдения было задействовано всего 11 портов, свободные 4 ушли на подключение двух офисным компьютеров и двух сетевых принтеров. Еще 4 порта ушли на подключение станций для официантов с системой Ico.

На роутере DIR 320 настроен динамический NAT. Преимущества данного способа перед статическим в первую очередь в безопасности и удобстве.

- Всякие злоумышленники не смогут определить по каким адресам доступны ваши серверы, т.к. их адреса будут все время меняться;
- Не нужно вручную назначать IP адреса, роутер сам распределит.

Так же на роутере поднят DHCP сервер, для того, чтобы устройства, отвечающие за открытие входной двери, имело доступ в интернет.

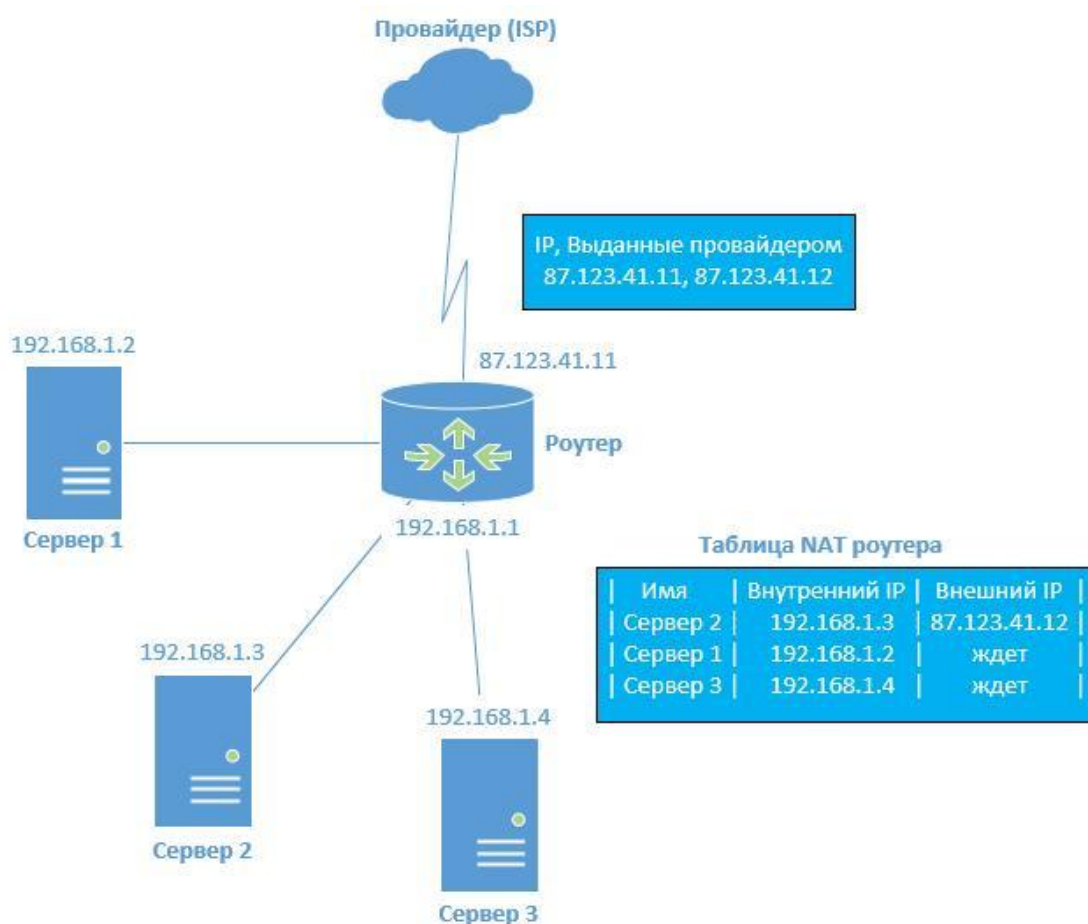


Рисунок 11 – схема развертки сети.

В данном примере провайдер выдал нам всего два внешних адреса: 87.123.41.11 и 87.123.41.12. В этом случае мы IP 87.123.41.11 назначаем роутеру, а оставшийся адрес будет автоматически отдаваться тому серверу, который первым попросит доступ в интернет (в данном примере это был сервер 2), остальные серверы будут ждать, когда первый закончит и этот IP адрес освободится.

3.6 Вход в ресторан

Пользовательская часть

1. Мы создаём сайт, на котором доступна регистрация
2. Пользователь заходит на сайт, входит при помощи профиля из социальной сети (FB/VK)
3. Если это известный профиль, то мы переводим пользователя на страницу, где показываем его коды для входа
4. Если это неизвестный профиль, то мы просим пользователя ввести его телефонный номер
5. На телефонный номер отправляется СМС
6. Мы просим пользователя ввести код из СМС, если он совпал, то переводим его на пункт 3

Система управления

1. У сайта есть система управления, в которой перечислены все зарегистрированные пользователи

2. Пользователей можно находить по именам, телефонам или использованным кодам
3. Пользователю можно запретить или разрешить вход
4. У пользователя можно посмотреть историю использования его кода для входа
5. Историю входов и использования системы за определённые периоды можно скачать в виде CSV файла

Система для замка

1. Для работы системы мы используем Raspberry Pi, камеру, цифровую клавиатуру и реле
2. Устройство выходит в интернет через Ethernet кабель (на раздающем роутере должен быть DHCP сервер для получения ip адреса и настроек)
3. Устройство скачивает базу актуальных кодов раз в X минут с сайта, для того, чтобы иметь возможность работать в случае отсутствия интернета
4. Пользователь может показать в камеру свой QR код или ввести цифровой код с клавиатуры
5. Устройство попытается проверить этот код через локальную базу, а затем и через API сайта
6. Если вход пользователя разрешён, то система замкнёт/разомкнёт реле для открытия замка

4 Опасные и вредные факторы при работе с ЭВМ

При работе с ЭВМ присутствуют в той или иной степени физические, химические, биологические и психофизиологические опасные и вредные факторы.

На пользователя могут воздействовать следующие физические опасные и вредные факторы:

повышение или понижение температуры в рабочей зоне;
высокий уровень шума на рабочем месте;
увеличение или уменьшение влажности;
увеличение или уменьшение подвижности воздуха;
повышенный уровень ионизирующего излучения в рабочей зоне;
высокое напряжение в электрической цепи, цепь, которая может произойти через тело человека;
повышенный уровень статического электричества;
повышенный уровень электромагнитного излучения;
увеличена напряженность электрического поля;
повышение интенсивности магнитного поля;
отсутствие или недостаток естественного света;
недостаточная освещенность рабочей зоны;
повышенная яркость света;
прямой и отраженной блескость;
повышенная пульсация светового потока.

Наличие химических опасных и вредных факторов в помещениях с компьютерами, в основном за счет широкого применения полимерных и синтетических материалов для внутренней отделки помещений, в

производстве мебели, ковров, электронных устройств и компонентов, систем питания, изоляционных элементов. Компьютерная технология производства предусматривает применение на основе лакокрасочных покрытий, красок, пластмасс. Когда компьютер нагревается, тем самым увеличивая концентрацию загрязнителей воздуха, таких как формальдегид, фенолы, полихлорированные бифенилы, аммиака, двуокиси углерода, озона, хлористого винила.

Группа биологических опасностей, которые могут привести к ухудшению заболевания или состояния здоровья пользователя, применяется повышенное содержание в воздухе патогенных микроорганизмов, особенно в комнате с большим количеством работы с недостаточной вентиляции во время эпидемий.

Психо-физиологические факторы, влияющие на пользователей, приводят к его физической и нервно-психической перегрузки. Характерным при работе с компьютером такая физическая перегрузка, так как длительное статическое напряжение мышц. Это вызвано вынужденном длительном сидении в той же позе, часто неудобно, необходимость постоянного мониторинга экрана (мышц напряженной шеи, ухудшение мозгового кровообращения), набор большого числа символов в смену (статический перенапряжение мышц плечевого пояса и рук). В то же время существует также локальная динамическая перегрузка пальцев и кистей рук. Статические мышцы от перенапряжения способствуют плохим эргономическим параметрам рабочего места и его компонентов (без подлокотников, пюпитра, FOOTREST), невозможность настроить параметры рабочего кресла и высота рабочей поверхности стола, неудобное расположение клавиатуры и дисплея, отсутствие регулируемых перерывов, несоблюдение специальных упражнений для снятия напряжения и расслабления групп мышц плечевого пояса, рук, шеи, спины и улучшить кровообращение.

Эти факторы представляют собой широкий спектр физических и психо-физических факторов, некоторые из которых по своим последствиям является

одноразовым (электрический ток, опасность пожара). Большинство факторов постоянно влияют друг и каждый пользователь компьютера. Эти факторы могут иметь как прямые, так и косвенные эффекты сложным образом от пользователя, негативные последствия которых проявляются как почти сразу, а постепенно, в течение долгого времени. Многие из факторов, которые, кажется, не имеет значения, в систематическом воздействии может привести к значительному снижению мощности и ухудшению состояния здоровья пользователя.

Для противодействия опасных и вредных факторов, организм использует адаптационно-компенсаторных реакций их функциональных систем, тратить жизненную энергию. Тем не менее, резервы организма и его возможности ограничены. Поэтому, накладывают ограничения на диапазон значений параметров отдельных факторов.

Чтобы уменьшить негативные последствия работы с компьютерами, следует выбрать рациональный режим труда и отдыха, использовать защитное оборудование, для проведения всестороннего оздоровления и профилактические меры (специальные упражнения, фортификацию, медицинский контроль). Безопасные условия труда на компьютере регулируют СанПиН 2.2.2 / 2.4.1340-03 "Гигиенические требования к персональным компьютерам и организации работы». Ответственность за выполнение этих правил, ответственность юридических лиц и индивидуальных предпринимателей, занятых в разработке, производстве и эксплуатации компьютеров, участвующих в проектировании и реконструкции помещений, предназначенных для использования с ПК.

4.1 Требования к работе в помещениях с ЭВМ

Микроклиматические параметры влияют на функцию человеческого деятельности, его благополучие и здоровье, а также надежность технологии вычислительного средства. Особенно большое влияние на климат является источником тепла в комнате. Основными источниками теплоты на дисплее залах: компьютеры, освещение устройства, обслуживаемые персоналом проводящей. Среднее значение тепловыделения составляет 310 Вт / м. Удельная значение выработки тепла от осветительных приборов 35-60 Вт / м. Количество тепла от обслуживающего персонала малых. Это зависит от количества работников в помещении и интенсивности выполняемой работы человеком.

Кроме того, общее выделение тепла зависит от внешних источников тепла дохода. Они включают в себя тепло, поступающее через окна усиления солнечного излучения тепла через непрозрачные конструкции ограждающие. Для того, чтобы создать нормальные условия для операторов компьютеров SET-Ленские климатические нормы (ГОСТ 12.1.005-88). Эти стандарты устанавливают оптимальные и допустимые значения температуры, относительной влажности и скорости движения воздуха в областях дисплея при условии явной избыток тепла, тяжесть работы и сезонов.

Таблица 6.1– Нормы температуры, относительной влажности и скорости движения воздуха в помещениях с ЭВМ

Температура наружного воздуха, град. С	Параметры воздушной среды на постоянных местах					
	Оптимальные			Допустимые		
	Температура, град. С	Относительная влажность, %	Скорость воздуха, м/с, не более	Температура, град. С	Относительная влажность, %	Скорость воздуха, м/с, не более
Ниже +10 Выше +10	20-22 20-25	40-60 40-60	0,2 0,5	18-22 Не выше 28	Не более 70 70 при 24 С 65 при 25 С 60 при 26 С 55 при 27 С 50 при 28 С	0,3 0,3

При оптимальных микроклиматических параметров обычно понимается таким образом, что в долгосрочной перспективе и систематического воздействия, чтобы обеспечить сохранение человеческого нормального функционального и теплового состояния организма без напряжения терморегуляции реакций, которые создают ощущение теплового комфорта и являются необходимым условием для обеспечения высокого уровня эффективности ,

Допустимые параметры микроклимата могут вызвать кратковременное и быстро нормализует указаний на функциональное и тепловое состояние терморегуляции тела и стрессовые реакции, без отклонения от физиологической адаптивной способности, не создавая нарушений здоровья, но вызывает неприятное ощущение тепла, ухудшение здоровья и снижение

эффективности.

Требования к освещению помещений с компьютерами

Правильно спроектированное и казнили освещение обеспечивает высокую эффективность, оказывает положительное психологическое воздействие на работников, повышает производительность труда. Важность этого вопроса для подсветки дисплея залов является тот факт, что большая часть информации (90%), оператор получает визуальный канал.

Для систем освещения предъявляются следующие требования:

- * квалификации работу соответствия света выполняемой характер зрительной работы;
- * достаточно равномерное распределение яркости в рабочем поверхностях и в прилегающих районах;
- * не резкие тени, вперед и не отражены блескость;
- * постоянство во времени освещения;
- * оптимальное направление освещения испускаемого светового потока приборами;
- * долговечность, эффективность, электрическая безопасность и пожарная безопасность, эстетика, удобство и простота использования.

В соответствии с действующим санитарным правилам и нормам 2.2.2 / 2.4.1340-03, искусственное освещение в помещениях для работы ПК должна быть общая единая система освещения. Промышленные и административные и общественные здания, в случае преимущественной работы с документами, необходимо применять комбинацию системы освещения (для общего освещения дополнительно установленные местные Светильники, предназначенные для освещения зоны расположения документов). Освещение на столе в области рабочего документа размещения должно быть 300 - 500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна превышать 300 люкс.

Следует ли ограничивать неравномерность яркости в распределении ПК пользователя, а соотношение яркости между рабочими поверхностями не

должно превышать 3: 1 - 5: 1, а между рабочими поверхностями и поверхностями стен и оборудования 10: 1.

Дисплей залы обычно используют одна сторона естественное освещение. Для того чтобы уменьшить солнечную инсоляцию светопроемы удовлетворены на север, северо-восток или северо-западной ориентации. Мониторы имеют подальше от окон и таким образом к окну на стороне. Если на экране дисплея окно, требует специальных экранирующих устройств (светорассеивающего шторы, регулируемые жалюзи, солнечная с покрывающей пленкой металлического).

Для искусственного пространства дисплея освещения лучше всего использовать люминесцентные лампы, так как они имеют высокую светоотдачу (до 15 лм / Вт и более), длительный срок службы (10000 часов), низкая яркость освещенной поверхности, близкой к естественной спектрального состава излучаемого света, что обеспечивает хорошую цветопередачу.

Наиболее подходит для отображения пространства являются люминесцентные лампы ЛБ (белый свет) и ЛТВ (теплый белый свет) мощностью 20, 40, 80 Вт.

Для устранения бликов экрана дисплея прямого светового потока светильников общего освещения особенность на стороне рабочего пространства, параллельно линии оператора и стеной окон. Такое расположение позволяет лампе производить их последовательное соединение в зависимости от естественного света и исключает раздражение глаз чередующимися полосами света и тени, которые возникают в поперечные расположения осветительных приборов.

4.2 Требования к рабочему месту оператора

Важную роль играет планирование рабочего места, которое должно удовлетворять требованиям простоты работы и экономии энергии и времени оператора, простота в обслуживании компьютеров, с соблюдением правил охраны труда. При планировании рабочего места необходимо учитывать охват рук в месте расположения дисплеев, клавиатуры компьютера. Эти зоны устанавливаются на основе антропологических данных человеческого тела. Наиболее удобным считается место, имеющий выемку соответствующую формировать бедра и наклон назад. Спинка кресла должна быть изогнута, плотно талии. Его длина 0,3 м и шириной 1 м OD, радиус изгиба 0,3 - 0,35 м. Движение оператора должно быть таким, чтобы группа его мышцы были загружены равномерно, но дополнительные накладные движения устранены. Во время работы оператор не должен подвергаться воздействию внешних раздражителей, которые могут быть мрачной живописи и компьютерный зал устройств. Таким образом, всеми необходимыми средствами, чтобы уменьшить усталость и стресс оператора ЭВМ, создавая атмосферу комфорта. Человек, вероятно, никогда не сможет полностью избежать вредного воздействия современных технологий, но мы можем свести его к минимуму. Большинство проблем решаются с правильной организации рабочего места, соблюдение правил техники безопасности и разумного распределения рабочего времени.

Электрические характеристики безопасности. Электроустановки, которые включают в себя практически все компьютерное оборудование, являются большой потенциальной опасности человека, так как в процессе эксплуатации или техобслуживания человек может коснуться частей под напряжением. Специфическая опасность электроустановок: токоведущим проводникам, жилищные стеллажами компьютеров и другого оборудования, под напряжением в результате повреждения (пробоя) изоляции, не подают каких-либо сигналов, которые предупреждают об опасности человека. Человеческий ответ на электрический ток возникает только при протекании последнего через тело человека. Экспериментальные

исследования показали, что человек начинает чувствовать себя раздражающим переменного тока промышленной частоты мощностью 0,6...1,5 мА постоянного тока и 5 ... 7 мА. Эти токи не представляют серьезной опасности для деятельности человеческого организма и потому, что при этом сила тока может освободить независимого человека от контакта с токоведущими частями, то это допустимо в течение длительного потока через человеческое тело.

В тех случаях, когда раздражающий ток становится настолько сильным, что человек не в состоянии освободиться от контакта свободный, существует опасность постоянного тока через тело человека. Длительное воздействие таких токов может привести к трудностям и дыхательной недостаточности. Для промышленной частоты переменного тока, не отпускающего ток находится в пределах 6 ... 20 мА или более. DC не вызывает эффект не отпускает, и приводит к сильной боли, сила тока 15 ... 80 мА или более. При протекании тока в несколько сотых Ампера разделить опасность работы сердца. Мерцательная аритмия может произойти, что является случайным, не координированному сокращению мышечных волокон сердца, и сердце не может вести кровь через сосуды, есть остановка сердца, с последующим полным остановки сердца. Как показали экспериментальные исследования выбрильятных пороговых токов зависят от массы тела, длительности протекания тока и его пути.

При нажатии любой из компьютерных элементов могут быть токи разряда статического электричества. Такие разряды не опасны для человека, однако, может привести к выходу из строя компьютера. Для уменьшения количества зарядов, возникающих в дисплейных залах, охватывающих технологии, используемые полов однослойный ПВХ антистатический линолеум марки АСН. Другим методом защиты является нейтрализация статического электричества ионизированный газ. Можно также применить общее и местное увлажнение воздуха.

требования

пожарной

безопасности

Помещение, в котором находится ПК, категории опасность пожара относится к категории "В". Как правило, существует большое количество потенциальных источников воспламенения, таких как кабельные линии, используемые для ПК источника питания от сети переменного тока напряжением 220 В, что для того, чтобы уменьшить горючесть огнезащитного покрова яйцекладки покрытием в металлических трубах. Электронный дисплей лучевая трубка, которая является взрывоопасной без дополнительной защиты, различных электронных устройств, которые в случае выхода из строя систем охлаждения может вызвать короткое замыкание, оборудование мебелью из горючих материалов; средств массовой информации, таких как бумага, магнитная лента.

Таблица 6.2 определена категория помещений в результате взрыва и пожара.
В таблице 6.3 Улучшение классов зон.

Таблица 6.2 – Таблица категорий помещений

Категория	Характеристика	Примечания
В Пожароопасная	Помещения, в которых находятся в обращении горючие и <u>трудногорючие</u> пыли, твердые горючие и <u>трудногорючие</u> вещества и материалы, способные только гореть при взаимодействии с водой, кислородом воздуха или между собой	Помещение характеризуется наличием веществ и материалов в указанных количествах

Возможно возникновение пожара, и, следовательно, необходимо предусмотреть меры по предотвращению пожаров: соблюдение требований пожарной безопасности при проектировании и эксплуатации систем

вентиляции в соответствии со СНиП 41-03-2003; соблюдение условий пожарной безопасности электрических установок в соответствии с SAE - 2002; наличие устройств отчетности :

- пожарные извещатели (линейные, тепловые, дымовые и т.д.);
- автоматические установки пожаротушения (газовые централизованного и модульного типа, углекислотные);
- инструкции по мерам противопожарной безопасности;
- план эвакуации людей и технических средств.

Таблица 6.3 — Классы зон помещений

Класс	Характеристика пожарной зоны
I — II	Зоны, расположенные в помещениях, в которых обращаются твердые горючие и <u>трудногорючие</u> вещества и материалы

Для улучшения условий пожарной безопасности в помещении установлен настил из негорючих материалов, технологически съемным. Бумага и лента хранится в металлическом корпусе. При наличии двух типов диоксида углерода огнетушителя ОУ-5, а также два детектора дыма. В случае пожара все сотрудники отображать залы должны знать порядок действий персонала в случае возникновения пожара:

- при возникновении пожара немедленно сообщить в пожарную часть по телефону 01;
- по возможности обесточить помещения;
- принять все зависящие меры по эвакуации людей;
- эвакуированных людей направлять в безопасные помещения;
- убедившись, что все люди эвакуированы, покиньте опасную зону и действуйте по указанию начальника или пожарников;
- по возможности приступите к тушению пожара с помощью огнетушителей, внутренних пожарных кранов и других подручных средств;

- если ликвидировать очаг горения своими силами невозможно, то следует выйти из помещения, закрыв за собой дверь, не запирая ее на замок;
- в задымленном помещении следует соблюдать меры безопасности (дышать через влажную ткань, прикрыв ею нос и рот);
- во избежание отравления дымом необходимо открыть окна в комнате;
- приступить к эвакуации имущества

В этом разделе дипломной работы были изложены требования к работе инженера - программиста. Созданные условия должны обеспечить удобную посадку. На основе изучения литературы по этому вопросу, мы получили оптимальный размер рабочего стола и стула рабочей поверхности и проведен выбор системы и расчет оптимального освещения производственных помещений, а также расчет уровня шума в рабочее место. Соблюдение условий, определяющих оптимальную организацию рабочего инженера - программиста, будет держать хорошую производительность в течение всего рабочего дня, увеличение совместно количественно и качественно производительности отношений программист, который, в свою очередь, будет способствовать быстрому развитию и отладки программного обеспечения.

Заключение

В рамках выпускной квалификационной работы, целью которой была

проектирование для достижения конкурентных преимуществ были решены поставленные задачи.

Изложены теоретические и правовые основы разработки систем безопасности. Систему безопасности можно разделить на физические, технические и комбинированные системы охраны. Технические системы охраны можно разделить на механические и электронные. Составной частью электронных систем охраны являются системы видеонаблюдения.

Проведен обзор современных архитектур систем видеонаблюдения и wi-fi сетей.

Рассмотрено современное состояние деятельности ресторана «Квартира Кости Кройца». Рассмотрено программное и техническое обеспечение предприятия.

Разработана система видеонаблюдения, wi-fi сеть, локальная сеть для ресторана «Квартира Кости Кройца». В результате анализа аппаратного и программного обеспечения, предлагаемого на рынке информационных технологий, разработан оптимальный вариант всех систем.

1. Конституция РФ от 12.12.1993 // СПС Консультант +
2. Гражданский кодекс 30 ноября 1994 года N 1-ФЗ// СПС Консультант +
3. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных"// СПС Консультант +
4. Бородулин, В. В. Управление передачей данных в системах беспроводного видеонаблюдения реального времени] : автореф. дис. канд. техн. наук : 05.13.01 / В. В. Бородулин. - Хабаровск, 2012. - 18 с.
5. Васин, Николай Николаевич. Расширение функциональных возможностей систем видеонаблюдения / Н. Н. Васин, Р. Р. Диязитдинов, В. Ю. Куринский. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2013. - 224 с.
6. Гвоздек, Михаэль. Справочник по технике для видеонаблюдения. Планирование, проектирование, монтаж / М. Гвоздек ; пер. с нем. Л. Н. Казанцевой. - Москва : Техносфера, 2014. - 543 с.
7. Дементьев А.Н. Электронные системы безопасности личности и имущества. Ч.2. Охранное телевидение: учебное пособие. - Томск: В-спектр, 2014 - 172 с.
8. Карташов Б.А. Компьютерные технологии и микропроцессорные средства в автоматическом управлении. - Ростов-н/Дону: Феникс, 2012.- 540 с.
9. Лыткин А. IP-Видеонаблюдение. Наглядное пособие. - Санкт-Петербург: ООО "Издательство "Авторская книга", 2014. - 200 с.
10. Меркишин Г. В. Системы наблюдения: новые принципы построения. — Москва: Издательство "Радиотехника", 2014. - 160 с.
11. Никулин, О. Ю. Системы телевизионного наблюдения [Текст] : учеб.-справ. пособие для учеб.заведений МВД РФ / О.Ю.Никулин,А.Н.Петрушин. - М. : "Оберег-РБ", 2014. - 176 с.
12. Обухова, Н. А. Методы видеонаблюдения, сегментации и сопровождения движущихся объектов : автореф. дис. д-ра техн. наук : 05.12.04 / Н. А. Обухова. - СПб., 2013. - 32 с.

13. Попов, А. Моя азбука видеонаблюдений / А. Попов. - СПб. : Алгоритм безопасности, 2013. - 246 с.
14. Селищев, В. А. Системы видеонаблюдения как средства охраны объектов информационной защиты : учебно-методическое пособие / В. А. Селищев, А. К. Талалаев, Н. Е. Проскуряков. - Тула : Издательство ТулГУ, 2014. - 113 с.
15. Смелков, В. М. Дискретно-аналоговые методы повышения информационной способности телевизионных камер и обнаружителей движения на ПЗС для промышленного видеонаблюдения и телевизионной охраны. - Великий Новгород, 2014. - 28 с.
16. Соловьева-Опошнянская, А.Ю. Видеонаблюдение как механизм обеспечения безопасности / Соловьева-Опошнянская, А.Ю. // Право и управление. XXI век. – 2015. - №2. – С. 140-143
17. Хамухин, А. В. Разработка и анализ высокоэффективных способов и алгоритмов автоматического сопряжения, синхронизации, юстировки изображений, управления поворотными камерами и обработки информации в приборах и системах видеонаблюдения. - М., 2015. - 23 с.
18. Андрейчиков, И. Мощные и надежные видеокамеры для наружного видеонаблюдения от компании Axis Communication s / И. Андрейчиков // Алгоритм безопасности.- 2013. - № 3.- С. 68.
19. Белов, В. Монтаж системы видеонаблюдения предприятия. Взгляд со стороны заказчика / В. Белов // Алгоритм безопасности. - 2013. - № 6.- С. 8-13.
20. Бурков, А. Обзор ПО для организации IP-видеонаблюдения на базе DiGiVi / А. Бурков // Алгоритм безопасности. – 2015. - № 6.- С. 70-71.
21. Ильницкая, С. Основные тенденции в видеонаблюдении в 2015 году / С. Ильницкая // F+S: Технол. безопас. и противопожар. защиты.- 2015. - № 1.- С. 36-38.
22. Новиков, П. Проектирование сетевых систем видеонаблюдения. Часть 1 / П. Новиков // PROSystem CCTV.- 2013. - № 6.- С. 52-65.
23. Смирнов, А. Как снизить затраты на серверы для системы IP-

- видеонаблюдения? / А. Смирнов // Системы безопас. – 2012. - № 5.- С. 101.
24. Солдатова, Г. Надежная IP-система за приемлемые деньги: возможно ли это? / Г. Солдатова // Системы безопасности.- 2014. № 6.- С. 159.
25. Степанова, Н. Пять интересных факторов об одной системе видеонаблюдения / Н. Степанова // Алгоритм безопасности. – 2014. - № 3.- С.
26. Беспроводные сети Wi-Fi: учебное пособие/ А.В Пролетарский и др. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2007. – 215 с.
27. С.С. Старцев: Модели распространения радиосигнала Wi-Fi [Электронный ресурс] – НГАСУ (Сибстрин) – Электрон. дан. – 7 с
28. Рудаков Д.В., Комагоров В.П. К вопросу о проектировании беспроводных локальных сетей WLAN [Электронный ресурс] – Доклады ТУСУРа, №2 (22). – Электрон. дан. – 2010. – 5 с.
29. Официальный сайт D-Link – Электрон. дан. – Режим доступа: <http://www.dlink.ru/>
30. Денисов Д.В.: Пакетные радиосети: Учебное пособие. – Е: УрТИСИ ФГОБУ ВПО «СибГУТИ», 2014.

