

Министерство образования и науки Российской Федерации
Филиал Федерального государственного автономного образовательного учреждения
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
в г. Нижневартовске

Кафедра «Информатика»

ДОПУСТИТЬ К ЗАЩИТЕ

И.о.зав.кафедрой «Информатика»
к.ф.-м.н, доцент

/ А.В.Ялаев

« ____ » _____ 2018 г.

Система видеонаблюдения и сетевое обеспечение в офисном помещении

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ ЮУрГУ-12.03.01. 2018.438.ПЗ ВКР

Консультанты
Экономическая часть

к.э.н., доцент

/А.В.Прокопьев/

« ____ » _____ 2018г.

Безопасность жизнедеятельности

к.ф.-м.н, доцент

/ А.В.Ялаев /

« ____ » _____ 2018 г.

Руководитель работы

/К.Г. Майфат /

« ____ » _____ 2018 г.

Автор работы

обучающийся группы НвФл 431

/Л.Р. Ибатуллин /

« ____ » _____ 2018г.

Нормоконтролер
старший преподаватель

/Л.Н.Буйлушкина/

« ____ » _____ 2018г.

Нижневартовск 2018

АННОТАЦИЯ

Ибатуллин Л.Р, Система видеонаблюдения и сетевое обеспечение в офисном помещении. – Нижневартовск: филиал ЮУрГУ, Информатика: 2018, 65 с., 25 ил., 10 табл., библиогр. список – 20 наим., 1 прил.

Данная выпускная квалификационная работа представляет собой описание разработки системы видеонаблюдения и сетевое обеспечение в офисном помещении.

Рассмотрен сравнительный анализ типов видеокамер. Показаны и описаны структурные схемы систем видеонаблюдения. Рассмотрены современные этапы развития видеокамер.

Проведен аналитический обзор современных камер видеонаблюдения, после чего сделан вывод о том, что по техническим характеристикам целесообразнее будет использовать купольный тип камер.

Рассмотрен принцип работы купольной камеры и коммутатора. На основе этого были разработаны функциональная, структурная схемы.

Подобрана линия связи между видеокамерами и коммутатором.

Рассчитан экономический эффект.

Охарактеризована безопасность жизнедеятельности

					12.03.01.2018.438 ПЗ ВКР					
<i>Изд.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подп.</i>	<i>Дата</i>	Система видеонаблюдения и сетевое обеспечение в офисном помещении	<i>В</i>	<i>К</i>	<i>Р</i>	<i>Лист</i>	<i>Листов</i>
<i>Разраб.</i>		Ибатуллин Л.Р.							5	65
<i>Проверил</i>		Майфат Р.Г.								
<i>Н.контр.</i>		Буйлушкина Л.Н.								
<i>Утвердил</i>		Ялаев А.В.								
						Филиал ФГАОУ ВО «ЮУрГУ (НИУ)» в г. Нижневартовске кафедра «Информатика»				

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	7
1 АНАЛИТИЧЕСКИЙ ОБЗОР.....	9
1.1 Сравнительный анализ типов видеокамер	9
1.2 Обзор линий связи	17
1.3 Сетевой коммутатор	21
2 ПОСТРОЕНИЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ	29
2.1 Выбор камеры видеонаблюдения.....	29
2.2 Выбор сетевого коммуникатора.....	32
2.3 Выбор канала связи.....	33
2.4 Функциональная схема и принцип ее работы.....	35
2.5 Структурная схема и принцип ее работы.....	36
2.6 Программное обеспечение.....	40
3 ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКИЙ РАЗДЕЛ	49
4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ.....	53
ЗАКЛЮЧЕНИЕ	62
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	63
ПРИЛОЖЕНИЯ	
ПРИЛОЖЕНИЕ А. КОМПАКТ-ДИСК	65

ВВЕДЕНИЕ

Новой технологией в организации охранных систем является IP-видеонаблюдение, позволяющие всегда быть в курсе событий, происходящих на объекте, из любой точки мира, что обеспечивается объединением интернета с системой видеонаблюдения. IP-видеонаблюдение в цифровом формате, это более высокое качество изображения, чем аналоговое, а также ряд других преимуществ, среди которых:

- более длительный безотказный срок эксплуатации;
- многофункциональность и удобство в использовании;
- более широкие возможности настройки, большой угол обзора камеры и возможность установить ее в любом месте;
- отличная обработка данных и удобное хранение их.

Видеонаблюдение – ключевой элемент в составе системы охраны и безопасности предприятия. Ее установка оградит материальные ценности организации от хищения, и способствует контролю над действиями персонала в помещениях офиса, производства и склада. А так же отследит передвижения клиентов и посетителей по территории объекта.

Функцию охраны предприятия можно технически разграничить на две части: круглосуточный контроль периметра ограждения и контроль передвижения по территории рабочих и грузового транспорта. С целью предотвращения прямых хищений производится: видеофиксация перемещения готовых изделий, охрана сырья и оборудования, видеоконтроль целостности упаковки и обеспечение полной комплектации при отгрузке. Сеть видеокамер может использоваться для мониторинга рабочего процесса с целью его рационализации и оптимизации. Наблюдение эффективностью использования рабочего времени сотрудниками организации приведет к повышению производительности труда и дисциплины. Мониторинг в роботизированных цехах позволит быстро реагировать на внештатные ситуации, сохраняя тем самым, работоспособность дорогостоящего

оборудования. А так же оградить производственный процесс от различных действий сотрудников, которые могут привести к аварии опасной для жизни участников производства. Предоставление видеоматериалов ответственным работникам для анализа и их использование для разбора внештатных ситуаций, разрешения спорных вопросов, приводит к необходимости сохранения видеозаписей, получаемых с камер и ведения продолжительного архива. Основные задачи, стоящие перед системой видеонаблюдения по степени детализации изображения можно обозначить как:

- обнаружение объекта наблюдения;
- распознавание;
- идентификация.

На выбор оборудования для решения каждой из обозначенных задач влияют такие факторы как расстояние до объекта, условия наблюдения (погодные, время суток, условия освещенности).

Последнее время перед видеонаблюдением все чаще ставятся задачи видеоаналитики – от простейшего распознавания движения в поле зрения камеры до автоматизированной идентификации личности или обнаружения оставленных предметов.

Целью выпускной квалификационной работы является разработка системы видеонаблюдения и сетевого обеспечения в офисном помещении.

Задачи выпускной квалификационной работы:

- 1) Провести обзор типов видеокамер и коммутаторов, способы передачи информации от видеокамер на рабочее место оператора.
- 2) Подобрать камеры видеонаблюдения, коммутатор и линию связи между видеокамерами и коммутатором. Рассмотреть структурную и функциональную схемы системы видеонаблюдения.
- 3) Охарактеризовать экономическую целесообразность проекта.
- 4) Охарактеризовать безопасность жизнедеятельности при работе с системой видеонаблюдения.

1 АНАЛИТИЧЕСКИЙ ОБЗОР

1.1 Сравнительный анализ типов видеокамер

Существуют следующие типы видеокамер:

- 1) модульные;
- 2) миниатюрные;
- 3) купольные;
- 4) корпусные;
- 5) гиросtabilизированные.

1.1.1 Модульные

Модульные, они же бескорпусные камеры видеонаблюдения представляют собой плату с закрепленным на ней объективом (Рисунок 1.1).



Рисунок 1.1 – Внешний вид модульной камеры

Такая конструкция одновременно может считаться и преимуществом, и недостатком модели. С одной стороны, модульные камеры можно устанавливать в корпус или термокожух нужной конфигурации или использовать для скрытого видеонаблюдения благодаря маленьким размерам. С другой стороны, электроника и оптика камеры ничем не защищены и не могут противостоять негативным воздействиям среды или человека при использовании их в качестве самостоятельного элемента системы наблюдения.

Параметры и функциональные возможности видеокамер приоритетно определяются:

- матрицей;
- схемой обработки сигнала;
- объективом.

Все эти компоненты в бескорпусном исполнении присутствуют, а значит, по характеристикам такие камеры потенциально ничем не уступают другим видам.

Вполне возможно может возникнуть вопрос о целесообразности дополнительных работ по сборке, герметизации и пр. Дело в том, что иногда нет возможности подобрать готовое изделие, соответствующее совокупности требований к техническим характеристикам и дизайну. Кроме того, при выходе из строя модуля его замена обойдется дешевле, поскольку достигается экономия на приобретении кожуха. А при повреждении последнего отсутствует необходимость покупки электронной части.

Можно также рассмотреть вопрос меньшей безболезненности модернизации, при наличии необходимости, по каким-либо причинам, изменения характеристик в лучшую сторону.

Естественно, нельзя сбрасывать со счетов возможность обеспечения скрытой установки бескорпусной камеры, поскольку небольшие размеры модуля позволяют сделать это достаточно просто.

Основные характеристики бескорпусных видеокамер:

– модульные камеры могут иметь цветную или монохромную матрицу, как правило, 1/3-дюймовую. Они обеспечивают запись видео в достаточно высоком разрешении. Для недорогих устройств этот показатель составляет около 420 ТВЛ, для более дорогостоящих – 700 ТВЛ;

– светочувствительность также будет отличаться в зависимости от ценовой категории оборудования, начиная от 0,1 Люкс, заканчивая 0,005 Люкс;

– камеры работают в режиме день/ночь. Для реализации такой возможности, как правило, устанавливаются цифровые инфракрасные (далее – ИК) фильтры;

– чаще всего оснащаются фиксированным объективом с фокусом 2,8 или 3,6 мм;

– диапазон рабочих температур от -10 до +50. [1]

1.1.2 Миниатюрные

Обладают маленькими размерами, нередко используются в зданиях и для скрытого наблюдения, имеют квадратный или цилиндрический корпус (Рисунок 1.2).



Рисунок 1.2 – Внешний вид миниатюрной камеры

Мини камеры обладают следующими преимуществами:

– имеют маленькие размеры, что позволяет вести скрытое наблюдение, так как заметить мини камеру очень сложно;

– миниатюрные камеры редко подвергаются разрушениям со стороны вандалов.

Единственным недостатком миниатюрных видеокамер наблюдения является их неспособность вести профессиональное видеонаблюдение, где очень важны точность цветопередачи и качественная оптика. В этом отношении они значительно уступают обычным видеокамерам. Также стоит обратить внимание, что в законодательстве некоторых стран предусмотрена ответственность за ведение скрытого видеонаблюдения, о чем также нельзя забывать. [1]

1.1.3 Купольные

Купольные видеокамеры на сегодняшний день являются одним из самых востребованных приборов на рынке видеонаблюдения. Главным положительным атрибутом этой видеокамеры является многофункциональность и внешняя непримечательность.

Купольные камеры – это камеры имеющие корпус в виде полусферы (Рисунок 1.3). Корпус может быть выполнен как из пластика, так и из металла. Во втором случае, камера считается антивандальной. Основным преимуществом купольных видеокамер – это неочевидно для наблюдаемого, направление обзора видеокамеры. Под основным прозрачным куполом располагается второй, как правило, черного цвета, реже серебристого.



Рисунок 1.3 – Внешний вид купольной камеры

Купольные камеры делятся на поворотные и стационарные.

Поворотные камеры видеонаблюдения, помимо параметров, присущих остальным камерам, характеризуются:

- величиной угла вращения в горизонтальной и вертикальной плоскостях;
- скоростью поворота;
- диапазоном изменения фокусного расстояния объектива;
- наличием определенного количества предустановок (фиксированных углов поворота, значений фокусного расстояния).

Купольные видеокамеры так же разделяются на несколько видов:

- купольные видеокамеры с фиксированным объективом и не имеют возможности регулировки фокусного расстояния, т.е. фокусное расстояние задано один раз, и оно является неизменным;
- купольные видеокамеры с вариофокальным объективом, т.е. объектив с фокусным расстоянием, изменяемым вручную – это особенно удобно, когда нет достоверных данных, о том в каких условиях будет использоваться видеокамера, т.е. на каком расстоянии будет находиться объект для наблюдения. Вариофокальный объектив обычно настраивают один раз при монтаже видеокамеры и в последующем уже не корректируют настройки. Обычно в

купольные камеры устанавливаются с вариофокальным объективом с фокусным расстоянием 4-9 мм либо 2,8-12 мм.

Если купольная камера устанавливается в помещении, то крепится на потолок таким образом, чтобы основание камеры находилось параллельно полу (горизонтально), если на улице – то на стене здания, ограждении или опоре при помощи специального кронштейна, сохраняющего горизонтальное положение основания.

По своим функциональным особенностям купольные устройства могут быть:

- с цветной матрицей;
- монохромные;
- с возможностью записи звука;
- с наличием ИК подсветки. ИК подсветка позволяет видеть наблюдаемый объект в полной темноте. В видеокамерах с ИК подсветкой может быть установлен механический ИК фильтр или электронная ИК коррекция. [2]



Рисунок 1.4 – Внешний вид купольной поворотной камеры

1.1.4 Корпусные

В системах видеонаблюдения корпусные камеры занимают одну из лидирующих позиций. В ряде случаев они могут не комплектоваться объективами, сетевыми адаптерами или кронштейнами.

Корпусные видеокамеры оснащаются как встроенными, так и сменными объективами. Последний вариант более востребован в профессиональных системах безопасности. Установка разных объективов дает возможность подобрать оптимальный вариант для различных задач, исходя из характеристик конкретного объекта.

В большинстве случаев корпусная камера видеонаблюдения комплектуется прибором с зарядовой связью (далее – ПЗС-матрица) высокой чувствительности. Это способствует получению детализированного видеоряда контролируемого объекта. Большинство камер имеет довольно широкие функциональные возможности. Система настройки позволяет изменить следующие параметры в автоматическом и/или ручном режиме:

- шумоподавление;
- маскирование;
- детекция движения;
- компенсация фоновой засветки и других.

Таким образом удастся легко настроить камеры в зависимости от ситуации.

Корпусная видеокамера, как правило, предназначена для установки в закрытых отапливаемых помещениях. Однако, видеокамера, помещенная в специальный термокожух, получает защиту от попадания влаги, пыли и может быть установлена на улице. За счет этого можно без проблем осуществлять видеомониторинг при самых неблагоприятных погодных условиях. Функциональные детали видеокамеры, размещенной в защитном термокожухе, не могут быть повреждены агрессивными воздействиями внешней среды.

Внешний вид корпусной камеры представлен на рисунке 1.5.



Рисунок 1.5 – Внешний вид корпусной камеры

1.1.5 Гиростабилизированные

Видеокамеры используются на подвижных объектах. Задачей камеры является получение стабилизированного изображения. Данное устройство может применяться для различных объектов, к примеру, трансформаторные подстанции, нефтегазовый сектор, мачты линии электропередач (далее – ЛЭП).

В основном используются для обзора местности, наблюдения за обстановкой, мониторинга чрезвычайных ситуаций, проведения поисковых работ, обнаружения объектов и измерения их координат. [2]

Внешний вид гиростабилизированной камеры представлен на рисунке 1.6.



Рисунок 1.6 – Внешний вид гиростабилизированной камеры

1.2 Обзор линий связи

1.2.1 Ethernet кабель (витая пара)

Витая пара – это особый вид сетевого кабеля. Его основу составляют одна или несколько пар изолированных, а также скрученных между собой проводников (от их количества зависит категория кабеля). Количество витков на определенную единицу длины минимальное, но достаточное для того, чтобы значительно уменьшить взаимные наведения при передаче сигнала. Сверху витая пара, как правило, покрыта защитной пластиковой оболочкой.

В последнее время этот вид кабеля связи стал самым распространенным при создании локальных и структурированных кабельных сетей. Это произошло благодаря его дешевизне и легкости прокладки.

Основным недостатком витой пары является значительное затухание сигнала (до уровня не распознаваемости) на расстояниях свыше 100 метров. Но этот недостаток легко ликвидируется с помощью повторителей.

В зависимости от того, есть защита или нет, а также ее качества, различают несколько видов кабелей созданных по этой технологии:

- неэкранированная витая пара (UTP) – не используется никаких дополнительных защитных приспособлений;
- экранированная витая пара (STP) – используется медная сетка;
- фольгированная витая пара (FTP) – используется алюминиевая фольга;
- экранированная фольгированная витая пара (SFTP) – используется медная сетка и алюминиевая фольга.

При этом в некоторых видах экранированного кабеля могут использовать защиту вокруг каждой пары. Такой вид экранирования обеспечивает значительно лучшую защиту от различного рода наведений, как внутренних, так и внешних.

Всего на данный момент существует около 15 категорий витой пары. Они нумеруются от CAT 1 до CAT 8.2. В большинстве случаев категория имеет прямую зависимость от количества используемых пар для передачи информации, а также от количества витков, которые используются на единицу длины. Категории кабеля четко описаны в Американском стандарте проводки в коммерческих строениях.

Опишем кратко каждую из категорий:

- CAT 1 – всем известный телефонный кабель. В нем используется только одна пара. Применяется исключительно для передачи голоса и создания подключений с помощью модема;
- CAT 2 – устаревший тип кабеля, состоящий из 2-х пар проводников. Он поддерживал передачу данных на скоростях менее 4 Мбит/сек. Часто использовали его в сетях token ring. Сейчас редко используется в некоторых телефонных сетях;
- CAT 3 – улучшенная версия предыдущего 2-х парного кабеля. Создана для обеспечения передачи данных на скоростях до 10 Мбит/сек. Сейчас очень часто продолжает встречаться в телефонных сетях;
- CAT 4 – еще один неиспользуемый на сегодня вид кабеля. Состоит из 4-х пар, имеет скорость передачи до 16 Мбит/сек;

- CAT 5 – именно кабели этой категории чаще всего и называют «витая пара» в классическом ее понимании. Состоит из 4-х пар. Скорость передачи варьируется от 100 Мбит/сек (используются 2 пары) до 1000 Мбит/сек (используются 4 пары);
- CAT 5e – улучшенная версия обычной 5 категории. Также состоит из 4-х пар. Кабель имеет те же скоростные характеристики, что и витая пара предыдущей категории. Сейчас эта категория является самой распространенной;
- CAT 6 – для передачи используется 4 пары, которые позволяют повысить скорость передачи до 10000 Мбит/сек;
- CAT 6a – для передачи используется 4 пары, которые позволяют повысить скорость передачи до 10 Гбит/сек;
- CAT 7 – для передачи используется 4 пары, которые позволяют повысить скорость передачи до 10 Гбит/сек. Кабель этой категории должен быть экранированным;
- CAT 8 – находится на данный момент в разработке. Предположительно позволит передавать информационный поток со скоростью до 40 Гбит/сек. Должен иметь общий экран или экран для каждой пары. [3]

1.2.2 Беспроводное подключение (Wi-Fi)

Развитие современных технологий придает значимость возможности предоставления удаленного доступа. Распространенное заблуждение, что сеть Wi-fi – это интернет. На самом деле – не так. Wi-Fi – протокол беспроводной сети, обеспечивающий прием и передачу информации между точками доступа и клиентами. Подключение Wi-Fi позволяет локально обмениваться информацией (пакетами данных), либо выходить в интернет – при наличии устройства.

Аббревиатура Wi-Fi разворачивается в «Wireless Fidelity», что дословно переводится, как «беспроводная точность». Придумывая термин, разработчики в рекламных целях использовали ассоциацию с «Hi-Fi», что переводится, как «высокая точность».

Широкое распространение с подачи разработчиков получила расшифровка: «высокая точность беспроводной передачи данных». На сегодняшний день от данной формулировки по ряду причин отказались и теперь «Wi-Fi» официально не означает ничего.

Минимально возможная скорость подключения: 0,1 Мбит/с. Максимально возможная реальная скорость подключения: до 54 Мбит/с. Максимально возможная теоретическая скорость подключения: до 600 Мбит/с.

Объединение устройств с поддержкой Wi-Fi обеспечивается посредством автономных точек доступа, либо управляемыми контролерами точек доступа или управляемых без помощи контроллеров точек доступа.

Плюсы Wi-Fi – отсутствие любых проводов для соединения. К одному Wi-Fi-роутеру одновременно возможно подключиться с нескольких устройств. Такая сеть устанавливается в тех помещениях, в которых нецелесообразно или невозможно провести обычную проводную сеть. Wi-Fi применяется во время проведения разнообразных конференций и международных выставок. Беспроводная сеть является лучшим решением в том случае, когда здание – это памятник архитектуры и в нем нельзя прокладывать провода кроме этого, Wi-Fi получил применение как для объединения компьютеров между собой и создания локальной сети, так и для подключения к Всемирной Паутине. Сейчас любой планшет и ноутбук имеет Wi-Fi-адаптер. То же касается и большинства телефонов. Подключиться можно везде, где есть сеть. Это делает такую технологию очень удобной. Раньше для подключения к сети были необходимы провода. Сейчас в интернет можно попасть где угодно при наличии Wi-Fi-сети. Будь то парк, кафе или аэропорт. Главное – наличие Wi-Fi-роутера. Очередной положительный момент беспроводной сети – это простота установки и легкость подключения. В случае нового устройства, подключенного к сети, все делается очень легко. Необходимо произвести простую настройку роутера. Так же желательно настроить безопасность и шифрование данных. Если же интернет только по проводам, то к каждому новому устройству нужно будет отдельно тянуть подключение. Из-за

этого офисы переходят с проводных сетей на беспроводные. Несмотря на все плюсы, минусы у такой сети тоже существуют. Серьезным недостатком беспроводной сети является зависимость скорости передачи данных от окружающей среды. Сети могут мешать препятствия (перегородки, зеркала, мебель и стены). Так же помехи может вызвать излучение от бытовых приборов. Кроме этого, на скорость соединения может повлиять стандартизация. Если одинаковые устройства выпущены разными производителями, это может вызвать проблемы с совместимостью. Скорость интернета зависит от создания сайтов, насколько они легковесные, а это уже зависит от разработчика. От среды зависит и радиус действия сети. Например, домашний роутер на улице может иметь зону покрытия в 450 метров, а в доме всего лишь 20-40. Если в одном помещении находятся два роутера, настроенных на работу в одном канале, то они будут мешать друг другу работать. Из-за этого может быть снижение качества и скорости соединения. Такая ситуация случается в многоквартирных домах, в которых много людей пользуются беспроводной сетью. У этой технологии немало недостатков, но все они компенсируются достоинствами. Это увеличивает популярность Wi-Fi с каждым днем. [3]

1.3 Сетевой коммутатор

Сетевой коммутатор (свитч) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты.

В процессе работы свитч анализирует MAC адреса всех подключенных устройств и создает специальную таблицу соответствия портов, что позволяет локализовать сетевой трафик.

В процессе проектирования системы IP-видеонаблюдения внимание уделяется соответствию технических характеристик коммутатора устанавливаемым камерам и общим требованиям к работоспособности сети.

1) Пропускная способность.

Любой сетевой коммутатор для видеонаблюдения обладает определенной пропускной способностью. Иначе говоря, это фактический объем данных, который оборудование может пропустить за единицу времени. При этом также учитывается пропускная способность каждого порта. Самые распространенные значения – 10/100 Мбит/с и 1 Гбит/с.

Нужно учитывать, что часто общая пропускная способность коммутатора может быть ниже, чем суммарное значение всех портов. Если подобное оборудование полностью загрузить, то система не сможет работать с должной эффективностью. Будут наблюдаться зависания изображения и периодическое отсутствие сигнала.

2) Количество портов.

Этот параметр определяют максимальное количество подключаемых камер. Для домашнего видеонаблюдения часто обходятся коммутатором с небольшим количеством портов (от четырех). Для профессиональных систем используются оборудование с 8-16-24 портами. Ориентируясь на количество портов, обязательно учитывают соответствие общей пропускной способности.

3) Исполнение.

Как и IP-камеры, коммутаторы могут изготавливаться для уличных и внутренних систем видеонаблюдения. Коммутаторы в уличном исполнении должны гарантировать работоспособность при любых климатических условиях. Поэтому оборудование выполняется в корпусах повышенной прочности со степенью защиты не ниже IP66.

Для систем, устанавливаемых внутри помещений, используется коммутатор для камер видеонаблюдения в стандартном исполнении. Популярностью

пользуются компактные модели с возможностью монтажа на DIN рейку, но они отличаются малым количеством портов.

4) Наличие PoE.

PoE (Power over Ethernet) – это технология для обеспечения питания удаленного оборудования посредством стандартного Ethernet кабеля. Наличие PoE существенно упрощает монтаж системы видеонаблюдения, т.к. питание подается по стандартному сетевому кабелю (витая пара). Важный момент – коммутатор с PoE используется с камерами, поддерживающими эту функцию (обязательно указывается в технических характеристиках). [4]

1.3.1 Коммутатор Ubiquiti UNIFI US-48-750W

Особенностью модели является усиленный блок питания. Ubiquiti UniFi Switch 48-750 предоставит пользователю 48 гигабитных Ethernet портов, а также 2 SFP и 2 SFP+ порта, которые позволяют подключать коммутатор к оптическим линиям связи. Весьма полезным качеством является поддержка двумя оптическими портами стандартов SFP+ со скоростью передачи данных до 10 Гб/сек. Коммутатор обладает вычислительной частью, которая обеспечивает обработку трафика в 70 Гб/сек. Важной особенностью коммутатора является поддержка передачи питания подключенным устройствам по стандартам POE+ IEEE 802.3af/at и 24VDC Passive PoE. Для этого Ubiquiti UniFi Switch 48-750 оснащен блоком питания мощностью 750 Вт. Этого будет более чем достаточно для питания как минимум нескольких десятков PoE клиентов.

Характеристики коммутатора и внешний вид Ubiquiti UNIFI US-48-750W представлены в таблице 1.1 и на рисунке 1.7. [5]

Таблица 1.1 – Характеристики коммутатора Ubiquiti UNIFI US-48-750W

Классификация	
Тип	коммутатор
Бренд	Ubiquiti UNIFI US-48-750W
Вид	управляемый
Размещение	монтируемый в стойку, настольный
Порты	
Базовая скорость передачи данных	10/100/1000/10G Мбит/сек
Общее количество портов коммутатора	52
Количество портов 100 Мбит/сек	48
Количество портов 1 Гбит/сек	48
Поддержка PoE	есть
Количество SFP-портов	4
Технические характеристики	
Внутренняя пропускная способность	70 Гбит/сек
Условия эксплуатации	
Рабочая температура	от -5°C до +40°C
Габариты, вес	
Ширина	485 мм
Высота	44.5 мм



Рисунок 1.7 – Внешний вид коммутатора Ubiquiti UNIFI US-48-750W

1.3.2 Коммутатор Cisco SG300-10MPP-K9-EU

Коммутатор предназначен для использования в малом и среднем бизнесе, обеспечивая надежную основу для совершения сетевых операций. Данный коммутатор обладает 8-ю портами PoE+ с бюджетной мощностью 124 Вт, 2-мя мини портами Gigabit Ethernet, а также снабжен такими необходимыми функциями, как повышение доступности критически важных приложений, защиты конфиденциальной информации и оптимизации пропускной способности сети для более эффективной передачи информации и приложений. Предлагает простое и безопасное подключение к сотрудникам, работающим в небольших офисах: как

между собой, так и со всеми серверами, принтерами и аналогичными устройствами, требующими беспроводного сетевого соединения. Питание посредством Ethernet делает данный коммутатор универсальным помощником для организации VLAN, допуская размещение в любом, удобном для пользователя месте без ограничений в приближенности к источнику электрической энергии. Благодаря высокому уровню безопасности соединения, данный коммутатор способен отделять служебный трафик от гостевых пользователей и предоставлять им отдельные трафики, тем самым, сохраняя приватность проводимых сеансов.

Характеристики коммутатора и внешний вид Cisco SG300-10MPP-K9-EU представлены в таблице 1.2 и на рисунке 1.8. [6]

Таблица 1.2 – Характеристики коммутатора Cisco SG300-10MPP-K9-EU

Классификация	
Тип	коммутатор
Бренд	Cisco SG300-10MPP-K9-EU
Вид	управляемый
Размещение	монтируемый в стойку
Порты	
Базовая скорость передачи данных	10/100/1000/ Мбит/сек
Общее количество портов коммутатора	28
Количество портов 100 Мбит/сек	28
Количество портов 1 Гбит/сек	28
Поддержка PoE	есть
Количество SFP-портов	2
Технические характеристики	
Размер таблицы MAC адресов	16384
Внутренняя пропускная способность	56 Гбит/сек
Скорость обслуживания пакетов	41,67 Mpps
Буфер пакетов	8 Мбайт
Условия эксплуатации	
Рабочая температура	от 0°C до +40°C
Рабочая влажность	от 5% до 90%, без конденсата
Потребляемая мощность	217 Вт
Габариты, вес	
Ширина	440 мм
Высота	44 мм
Глубина	257 мм
Высота	44 мм
Вес	3,95 кг



Рисунок 1.8 – Внешний вид коммутатора Cisco SG300-10MPP-K9-EU

1.3.3 Коммутатор HPE V1910-24G-PoE+ JG539A

Эти устройства идеально подходят для сред, где требуется точное управление, а также гибкость и интеллектуальные функции для простоты настройки и администрирования сети. Устройства серии 1910 – это простые в администрировании коммутаторы с интеллектуальным управлением, фиксированной конфигурацией и расширенным набором функций. К настраиваемым функциям коммутаторов относятся базовые функции уровня 2, такие как виртуальные локальные сети (VLAN) и агрегирование каналов, а также более сложные функции, как например статическая маршрутизация уровня 3 и списки управления доступом.

Характеристики коммутатора и внешний вид HPE V1910-24G-PoE+ JG539A представлены в таблице 1.3 и на рисунке 1.9. [6]

Таблица 1.3 – Характеристики коммутатора HPE V1910-24G-PoE+ JG539A

Классификация	
Тип	коммутатор
Бренд	HPE V1910-24G-PoE+ JG539A
Вид	настраиваемый
Размещение	монтируемые в стойку
Порты	
Базовая скорость передачи данных	24
Общее количество портов коммутатора	24
Количество портов 100 Мбит/сек	2
Количество портов 1 Гбит/сек	есть
Поддержка PoE	24
Количество SFP-портов	2
Технические характеристики	
Размер таблицы MAC адресов	16384
Внутренняя пропускная способность	8.8 Гбит/сек
Скорость обслуживания пакетов	6,6 Mpps
Буфер пакетов	512 Кб
Условия эксплуатации	
Рабочая температура	от 0°C до +40°C
Рабочая влажность	от 10% до 90%, без конденсата
Потребляемая мощность	220 Вт
Ширина	442 мм
Высота	44 мм
Глубина	238 мм
Вес	3,3 кг



Рисунок 1.9 – Внешний вид коммутатора HPE V1910-24G-PoE+ JG539A

Выводы по разделу один:

В данном разделе рассмотрены существующие типы видеокамер и коммутаторов, наиболее распространенные способы передачи информации от видеокамер на рабочее место оператора.

2 ПОСТРОЕНИЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

2.1 Выбор камеры видеонаблюдения

При выборе вида камеры видеонаблюдения необходимо учитывать следующие факторы:

- качество съемки;
- стоимость видео камеры;
- поддержка PoE;
- функция ночной съемки;
- стойкость к механическому воздействию.

В данной выпускной квалификационной работе (далее – ВКР) рассматривались следующие виды камер видеонаблюдения:

- модульные;
- миниатюрные;
- купольные;
- корпусные;
- гиросtabilизированные.

Гиросtabilизированные видеокамеры в основном используются на подвижных объектах, их задачей является получение стабилизированного изображения. Т.к. это свойство камер значительно увеличивает их стоимость и ввиду того, что данная функция нам не требуется, то использование данного типа камер не будет обосновано в нашей работе.

Модульные камеры имеют значительно меньшую стоимость по сравнению с гиросtabilизированными, так же они имеют достаточно хорошее качество видеосъёмки и могут быть оборудованы ИК датчиком для ночной съемки. В модульных камерах может присутствовать функция PoE, но использование данного типа камер будет затруднительно, т.к. они не имеют защитного кожуха и

поэтому установка их на улице не представляется возможной. Следовательно, использование данного типа камер в нашем проекте также исключается. [7]

Миниатюрные камеры в отличие от модульных имеют защитный корпус и также, как и модульные могут использоваться для ночной съемки и имеют функцию PoE. Но главным недостатком таких камер является плохая цветопередача, а также менее хорошее качество съемки.

Купольные камеры сочетают в себе все преимущества рассмотренных камер. Они могут использоваться для записи в темное время суток, имеют функцию PoE, позволяют вести запись в достаточно хорошем качестве и по стоимости близки к аналоговым. Плюс ко всему, имея форму купола, данный вид камер видеонаблюдения обеспечивает их защиту от физического воздействия. Класс защиты позволяет использовать их как в помещениях, так и на улице.

Корпусные камеры видеонаблюдения, так же как и купольные имеют функцию PoE, позволяют вести съемку в темноте, имеют небольшую стоимость, класс их защиты допускает использование данных камер, как в помещении, так и вне помещений. Но корпусные камеры более подвержены физическому воздействию и вандализму.

Сравнив все виды рассмотренных камер видеонаблюдения, наиболее подходящей для наших целей можно считать купольные камеры. Они сочетают в себе все преимущества, лишены недостатков присущих другим видам камер и полностью соответствуют нашим требованиям.

Для реализации проекта будут использоваться купольные камеры Amatek AC-IDV203VA. Данные камеры полностью удовлетворяют нашим требованиям, хорошо переносят как жару, так и холод и имеют небольшую стоимость.

Внешний вид камеры Amatek AC-IDV203VA представлен на рисунке 1.10. [8]



Рисунок 1.10 – Внешний вид камеры Amatek AC-IDV203VA

Технические характеристики Amatek AC-IDV203VA (2,8-12):

- габариты: 131×131×93 мм;
- масса: 0,70 кг;
- разрешение: 2 Мп;
- объектив: 2,8-12 мм;
- ИК подсветка: 30 м;
- основной поток: 1920×1080 25к/с;
- электронный затвор (AES) 1/25 - 1/10000 сек;
- детектор движения;
- режим «День/Ночь»;
- механический ИК-фильтр (ICR);
- сетевой интерфейс 1 RJ45 (влагозащищенный), 10М/100М Ethernet;
- поддержка PoE (Power over Ethernet);
- питание IP видеокамеры DC 12 В ± 10%;
- класс защиты IP66;
- размеры IP видеокамеры: диаметр 131×93 мм;
- корпус IP-видеокамеры металл, антивандальный корпус;
- рабочая температура -40 ... +60 °С. [9]

2.2 Выбор сетевого коммутатора

При выборе сетевого коммутатора необходимо учитывать следующие факторы:

- стоимость оборудования;
- количество портов для подключения камер;
- условия эксплуатации оборудования;
- скорость передачи данных;
- поддержка PoE.

В данной ВКР рассматривались следующие виды сетевых коммутаторов:

- коммутатор Ubiquiti UNIFI US-48-750W;
- коммутатор Cisco SG300-10MPP-K9-EU;
- коммутатор HPEV1910-24G-PoE+ JG539A.

Скорость передачи данных всех рассмотренных сетевых коммутаторов удовлетворяет нашим потребностям, т.к. используется относительно небольшое количество камер видеонаблюдения.

Условия эксплуатации оборудования так же не имеют критического значения при выборе оборудования, т.к. коммутатор будет находиться в помещении с нормальными условиями, следовательно, перепады температуры и относительной влажности не смогут навредить оборудованию.

Так же стоит отметить, что все перечисленные коммутаторы обладают поддержкой питания камер, т.е. PoE. Это позволит сэкономить на дополнительном питании для камер видеонаблюдения, т.к. уходит необходимость в приобретении источников питания для камер, а также в прокладке дополнительных кабелей.

Коммутатор Ubiquiti UNIFI US-48-750W обладает наибольшим количеством портов для подключения видеокамер, но такое количество портов является избыточным для нашего проекта. К тому же наибольшее количество портов делает данный коммутатор наиболее дорогим по стоимости.

Коммуникатор Cisco SG300-10MPP-K9-EU имеет меньшее количество портов, но так же, как и коммуникатор Ubiquiti UNIFI US-48-750W обладает высокой стоимостью, что делает его непривлекательным для нас.

Коммуникатор HPEV1910-24G-PoE+ JG539A имеет наименьшую стоимость среди представленного оборудования. Но, несмотря на лучшую цену, данный коммуникатор обладает всеми необходимыми нам характеристиками. Он поддерживает функцию PoE, имеет хоть и не лучшую, но достаточную скорость передачи данных, а также способен работать с 24 камерами видеонаблюдения, что полностью покрывает наши потребности и к тому же, обеспечивает резерв, на случай если в дальнейшем будут устанавливаться дополнительные камеры видеонаблюдения.

Исходя из всего выше сказанного, коммуникатор HPEV1910-24G-PoE+JG539A в наибольшей степени подходит в данном проекте. [10]

2.3 Выбор канала связи

При выборе канала связи между камерой видеонаблюдения и сетевым маршрутизатором необходимо учитывать ряд факторов:

- удаленность камеры видеонаблюдения от сетевого маршрутизатора;
- стоимость прокладки канала связи;
- наличие возможности прокладки того или иного канала связи;
- устойчивость канала связи к помехам.

В данной ВКР рассматривались следующие варианты каналов связи:

- Ethernet кабель (витая пара);
- неэкранированная витая пара UTP;
- фольгированная витая пара FTP;
- экранированная витая пара STP;
- фольгированная экранированная витая пара S/FTP;
- незащищенная экранированная витая пара SF/UTP;

– беспроводное подключение (Wi-Fi). [11]

Неэкранированная витая пара (UTP) имеет наименьшую стоимостью по сравнению с остальными видами кабелей. Но не обладает дополнительной защитой против помех, шумов и наводок. А т.к. канал связи между камерами видеонаблюдения и сетевым коммутатором может пролегать возле силовых кабелей, и иметь значительную протяжённость, следовательно, использование данного вида кабеля не может считаться предпочтительным.

Экранированную витую пару STP, фольгированную экранированную витую пару S/FTP, а также незащищенную экранированную витую пару SF/UTP использовать в данном проекте мы тоже не будем. Данные виды кабелей хоть и обладают необходимыми характеристиками в плане помехозащищенности, но это является также и минусом, так как их слишком большая, и не требуемая в данном случае помехозащищенность, оказывает непосредственное влияние на их стоимость.

Фольгированная витая пара FTP сочетает в себе как достаточную защищенность от разного вида помех и наводок, так и низкую стоимость, что поможет уменьшить конечную стоимость всего проекта.

Беспроводное подключение Wi-Fi обладает неоспоримым преимуществом по сравнению с кабелями разных типов. Такой вид связи камер видеонаблюдения с коммутатором в разы облегчает, а самое главное ускоряет процесс построения системы видеонаблюдения. Так же экономятся значительные денежные ресурсы на кабелях. Необходимо отметить и тот факт, что исключается шанс обрыва или умышленной порчи кабелей соединяющие камеры с коммутатором. Но, несмотря на все эти преимущества, беспроводные сети обладают и серьезным недостатком, который не позволяет использовать их в данном проекте. Этим недостатком является плохая проницаемость через толстые железобетонные стены.

Исходя из выше описанного, фольгированная витая пара FTP является наиболее оптимальным вариантом в данном проекте. [12]

2.4 Функциональная схема и принцип ее работы

Функциональная схема системы видеонаблюдения представлена на рисунке 2.1.

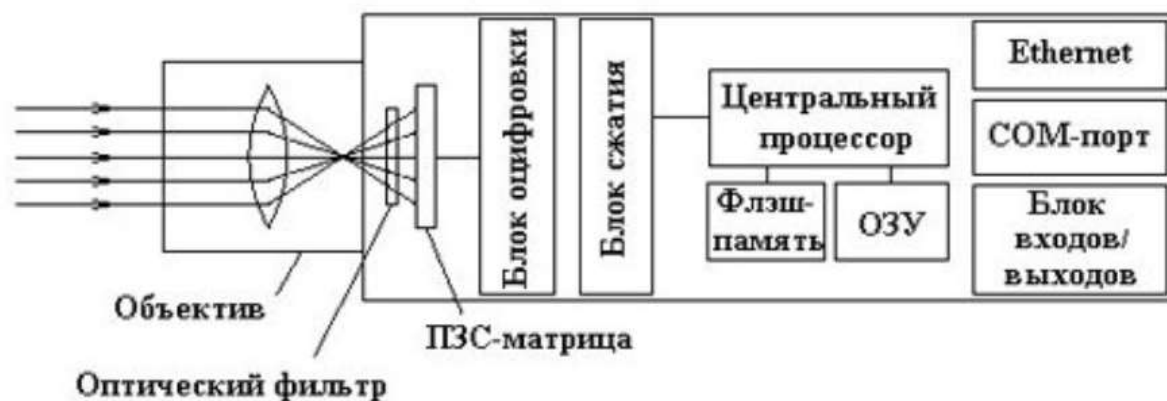


Рисунок 2.1 – Функциональная схема системы видеонаблюдения

Объективы видеокамер состоят из системы оптических линз, которая фиксирует световое изображение на ПЗС-матрице.

Световой поток формируется за счёт проецирования на светочувствительной ПЗС-матрице. Для точной, качественной цветопередачи, перед попаданием на ПЗС-матрицу, светопоток проходит через оптические отсекающие ИК фильтры которые входят в состав объектива. Фильтра представляют собой плоско – направленные параллельные, светопропускающие пластинки.

Светочувствительная матрица видеокамеры выполняет роль фотоприёмника, и является одной из главных составляющих схемы камеры видеонаблюдения, благодаря которой формируется выходное изображение.

Матрица – это прямоугольная полупроводниковая пластина, преобразующая световой поток, полученный от объектива, в электрический заряд, который передаётся на процессор для обработки, усиления, формирования видеосигнала. Светочувствительный прибор с зарядовой связью имеет соотношение сторон 4:3,

сформирована из огромного числа светочувствительных элементов – пикселей. Чем больше число пикселей содержит матрица, тем лучше качество картинка.

DSP (процессор обработки видеосигнала) – производит преобразование электронных зарядов, полученных с ПЗС-матрицы, в цифровой формат, что подходит для трансляции на экраны мониторов или записи. Процессор обрабатывает электронные заряды с каждого пикселя по отдельности, в режиме реального времени, путём анализа, определения наилучшего времени экспозиции, корректировки кадра. Таким образом, формирование выходного изображения происходит частично от каждого пикселя, при условиях индивидуальной освещённости, с дальнейшим соединением в единую картинку.

Оперативно запоминающее устройство служит временным хранилищем данных, которые находятся в процессе обработки процессором.

Флэш-память хранит редко изменяемые данные, например, настройки режимов съёмки, а также прошивку, управляющую работой IP видеокамеры.

Сетевой интерфейс необходим для передачи сформированного, сжатого видеоизображения по локальной сети или Интернету. Проводной интерфейс представляет собой модуль с Ethernet портом, для соединения камеры видеонаблюдения с компьютером, роутером, сервером, коммутатором. [13]

2.5 Структурная схема и принцип ее работы

Основными компонентами систем сетевого видеонаблюдения являются сетевая камера, видеокодер или видеосервер (применяется для подключения аналоговых камер), сеть, сервер и система хранения, а также программное обеспечение (далее – ПО) для управления системой видеонаблюдения и записи видеoinформации. Сетевые камеры и видеокодеры созданы на базе цифровых (компьютерных) технологий, поэтому они обладают возможностями, недоступными аналоговым камерам. Сеть, системы хранения и серверы –

стандартное ИТ – оборудование. Способность использовать обычное сетевое оборудование – одно из главных преимуществ сетевого видео.

Типовая структурная схема системы видеонаблюдения представлена на рисунке 2.2.



Рисунок 2.2 – Типовая структурная схема системы видеонаблюдения

Система состоит из следующих основных элементов:

- сетевые камеры, которые устанавливаются на удаленных объектах, причем на объекте можно установить 1 или несколько камер, в зависимости от размера объекта;
- центральный сервер, на котором установлено ПО для централизованного управления мониторинга всеми камерами, а также для записи информации, получаемой с камер;
- опционально можно установить дополнительные компьютеры в регионах, например, для локального наблюдения за объектом.

Задачи, которые позволяет решить данная система:

- централизованное наблюдение за несколькими объектами в режиме реального времени с возможностью одновременной записи изображения на сетевое хранилище;
- централизованное наблюдение за работой сотрудников в филиалах (офисах, магазинах, на складах), которые удалены от центрального офиса на сотни и тысячи километров;
- возможность централизованной записи видео по тревожному сигналу или в постоянном режиме;
- уведомление по телефону или на e-Mail при тревожном событии;
- возможность подключения удаленных рабочих мест для просмотра видео, а также просмотр видео с мобильного телефона (смартфона).

Принцип их действия состоит в том, что такие камеры производят захват, сжатие в форматы MPEG-2, MPEG-4, M-JPEG, и после этого совершают передачу со скоростью до тридцати изображений в секунду живого изображения по сети. IP-камеры дают возможность авторизованным пользователям получать и просматривать данные изображения, обрабатывать информацию, анализировать её и сохранять. При подключении камеры ей присваивается IP-адрес, т.е. она обладает возможностями веб-сервера, FTP-сервера, FTP-клиента, SMTP-клиента – возможность передачи информации посредством электронной почты, обработки сигналов тревоги и программирования. IP-камера по сети может передавать не только видеоизображение, но и другую информацию, такую как оцифрованный аудиосигнал, уведомление о тревоге или же обнаружении движения. Также, при помощи камер можно получить необходимые данные для возможности направления их в нужную сторону. Это касается поворотных камер.

Для нашего объекта структурная схема представлена на рисунке 2.3.

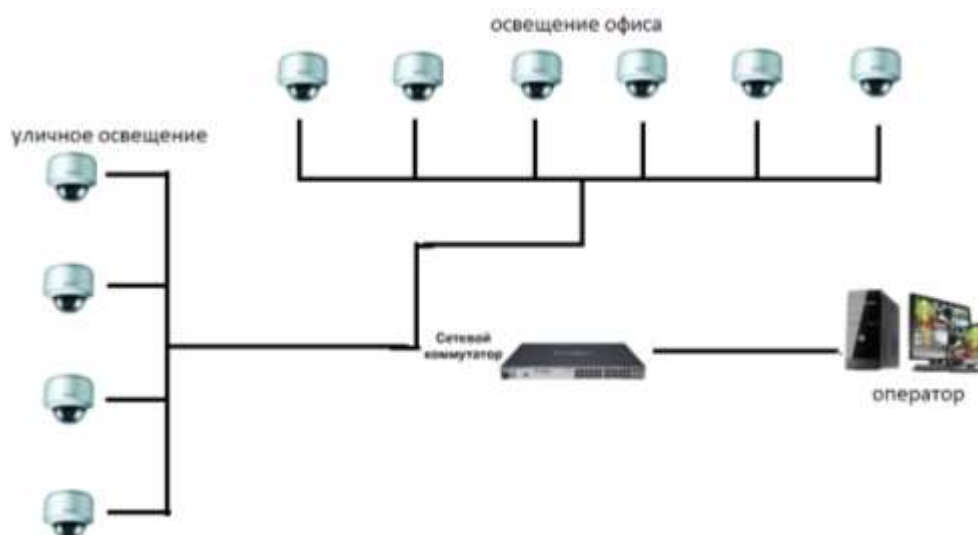


Рисунок 2.3 – Структурная схема системы видеонаблюдения

Система видеонаблюдения состоит из 10 купольных камер, 4 из которых находятся на улице и занимаются съемкой входа в офис и парковки, 6 камер расположены в офисных помещениях. В качестве канала связи используется фольгированная витая пара FTP. Сигнал от камер по витой паре поступает на сетевой коммутатор. С сетевого коммутатора информация поступает на компьютер оператора. Оператор на мониторе может просматривать запись с камер, как в реальном времени, так и из архива. На компьютере оператора имеются два жестких диска емкостью по 4 Тб, на которые идет запись со всех камер видеонаблюдения, а также производится резервное копирование, что обеспечивает большую безопасность. Объем жестких дисков позволяет хранить архивы видеозаписей до полугода. Когда жесткий диск полностью заполняется, происходит автоматическое удаление самых первых видеозаписей. Также со своего рабочего места оператор может задавать расписание записи видеокамер. При необходимости съемку в реальном времени можно включить на мобильном телефоне или другом компьютере. [14]

2.6 Программное обеспечение

После установки камеры необходимо настроить несколько ее параметров для корректной работы. Эти параметры включают: IP-адрес, sub-маску подсети, номер порта, и т.д. и могут быть установлены несколькими методами, 2 из которых:

- установка параметров камеры, используя браузер IE;
- установка параметров камеры, используя ПО камеры.

2.6.1 Настройка при помощи Web-браузера

По умолчанию, IP-адрес камеры: 192.0.0.64 , порт 8000 as the default port, admin – логин администратора, и 12345 – пароль администратора.

Для подключения к IP-камере введите ее IP в адресную строку браузера, появится окно «Login» (Рисунок 2.4). Введите имя пользователя (Account), пароль (Password) и нажмите «Login» для входа.

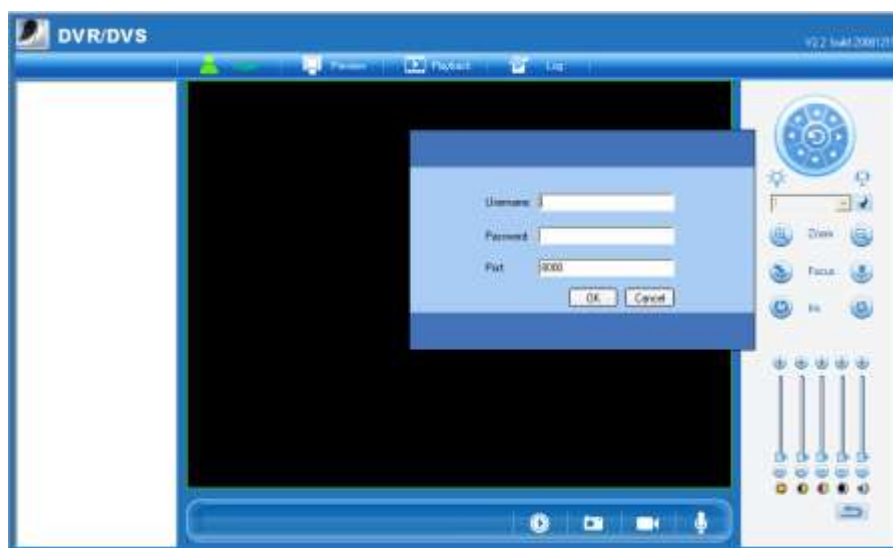


Рисунок 2.4 – Вход в настройки камеры через браузер

После удачной идентификации пользователя как администратора открывается меню камеры (Рисунок 2.5). При двойном нажатии на «Camera 01» или «Preview» для предпросмотра видео. Выберите «Camera 01» и «Main Stream», «Sub Stream» или «Open sound» для настройки. Укажите «Open sound» если Вы подключены к камере.



Рисунок 2.5 – Предпросмотр функционала камеры

Функции «Playback» (Воспроизведение) и «Log» (Список событий) доступны только при установке в камеру SD-карты. Для установки параметров камеры через браузер, выберите «Config» для входа в окно «Remote Parameters Config», в котором Вы осуществляете все необходимые параметры, как представлено на рисунке 2.6. Выберите необходимую для изменения функцию, нажав на нее (клавишей мыши). Нажмите IRIS+ для входа в подменю. Меню для удобства выполнено в виде графических настроек.

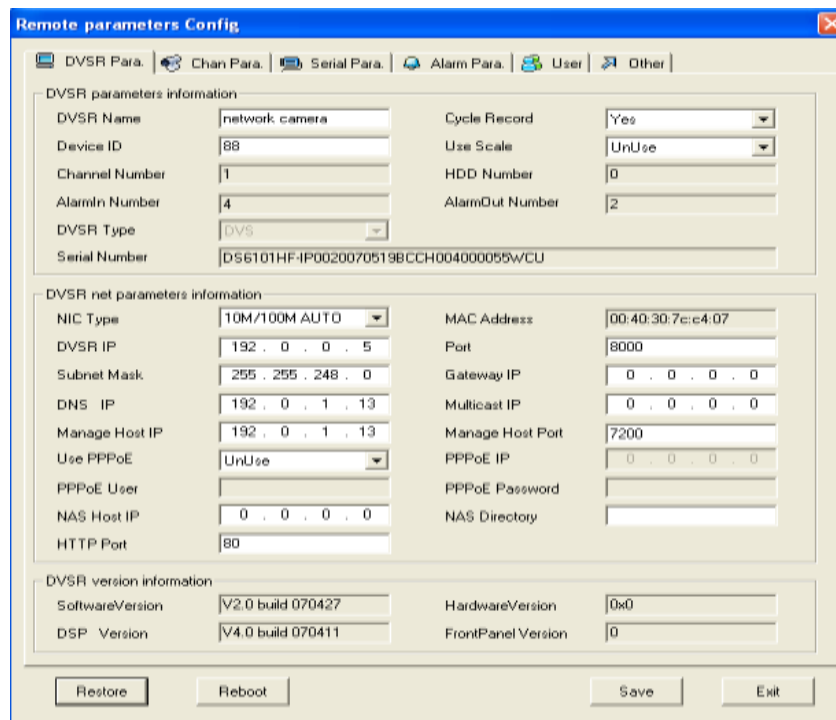


Рисунок 2.6 – Интерфейс настройки камеры

Настройки через Web - браузер являются достаточно сложными. Если появляются дополнительные вопросы по настройкам IP-видеокамеры через Web-браузер, можно воспользоваться справкой, находящейся на компьютере по адресу «Start» → «Program» → «Client Software 4.01». Данная справка появляется на компьютере после установки ПО IP-камеры.

2.6.2 Настройка через программное обеспечение

Для установки параметров камеры, используется бесплатное ПО Client Software-4000(v2.0).

После установки ПО устройства, на экране Вашего компьютера появится ярлык «Client Software-4000(v2.0)». Нажмите дважды на ярлык для входа в меню регистрации администратора «Register Administrator» (Рисунок 2.7). Пароль должен состоять более чем из 6 знаков.

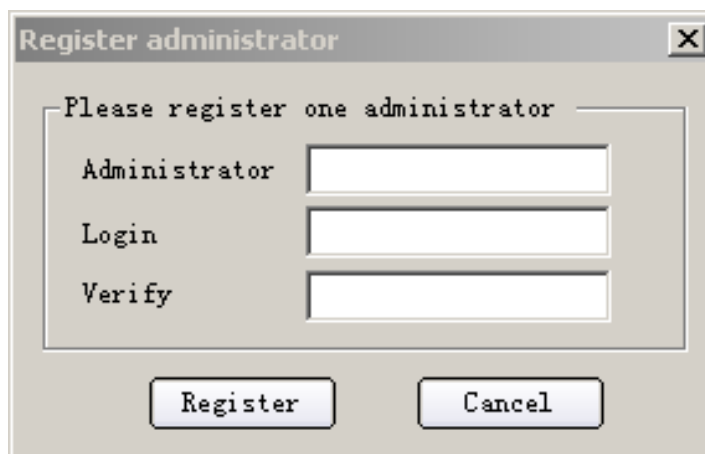


Рисунок 2.7 – Регистрация администратора системы

После ввода Имени администратора и пароля, на экране появится окно ввода для входа в программу (Рисунок 2.8). Введите зарегистрированные имя пользователя и пароль в окне. Нажмите «Login» для входа в программу.

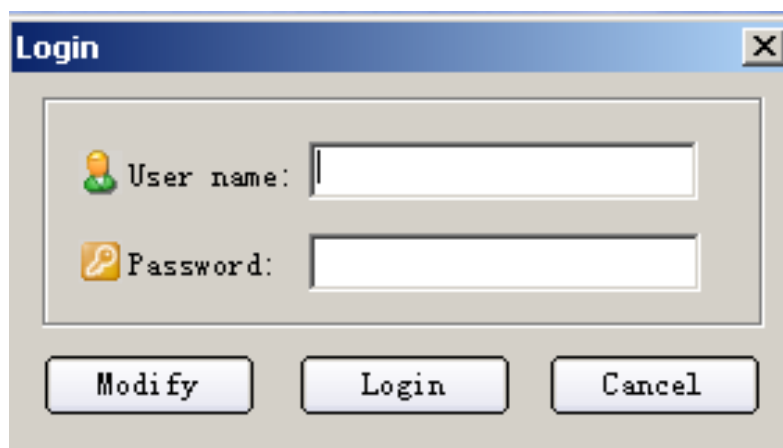


Рисунок 2.8 – Ввод имени и пароля пользователя

Следует хранить логин и пароль в безопасном месте, помнить, что доступ в программу просмотра и управления IP-видеокамерой осуществляется только с паролем.

После выполнения всех предыдущих операций открывается основное меню настройки камеры (Рисунок 2.9).

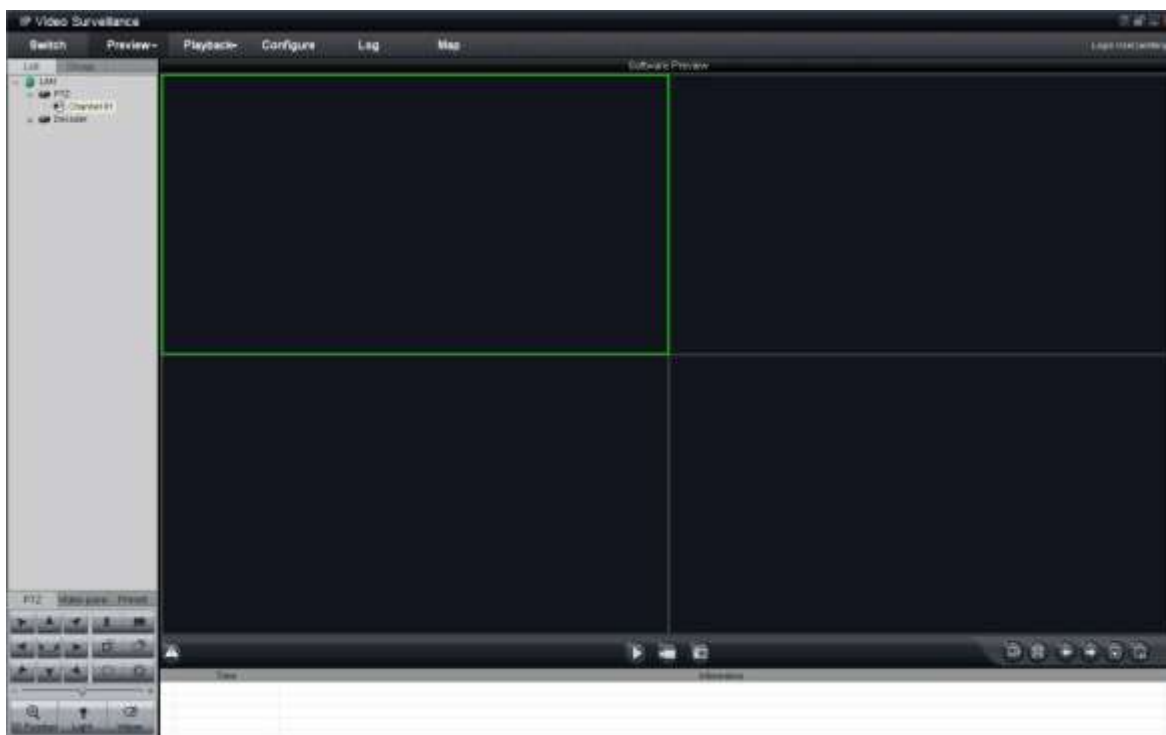


Рисунок 2.9 – Меню основной программы

При нажатии «Configure» (Рисунок 2.10) и правой кнопки мыши на свободном месте программы, выбирается «Add Area» для доступа в меню добавление зоны.

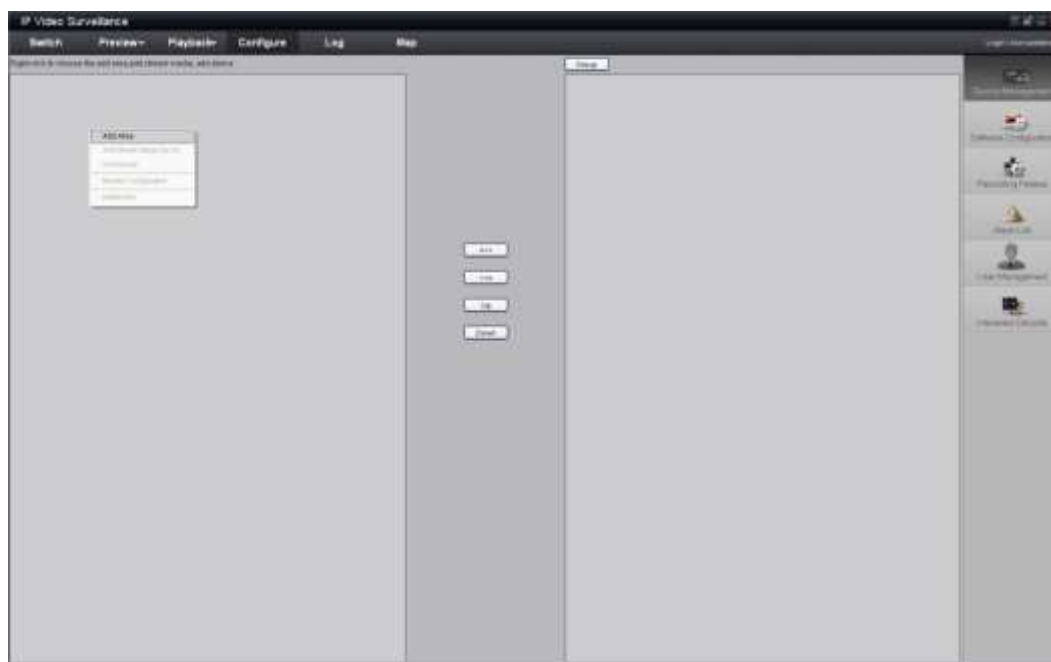


Рисунок 2.10 – Добавление зоны

Введите имя зоны, нажмите «ОК» (Рисунок 2.11), а затем на правую кнопку мыши для входа в меню (Рисунок 2.12).

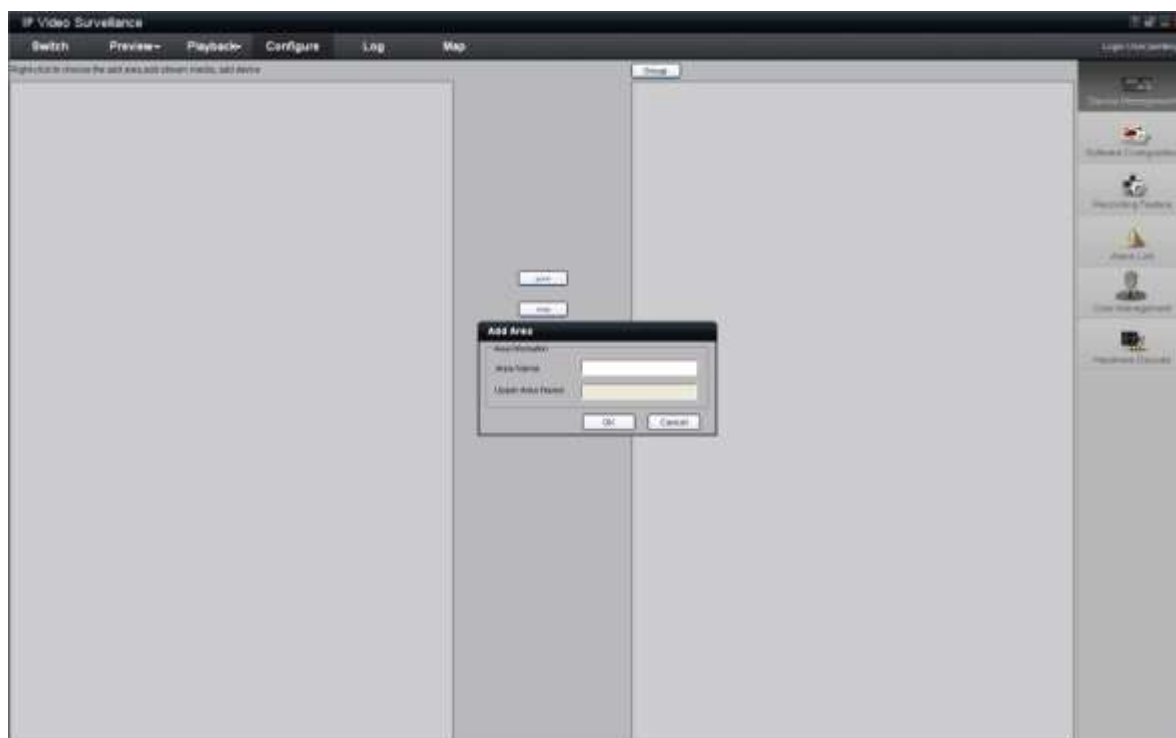


Рисунок 2.11 – Вход в меню добавления зоны

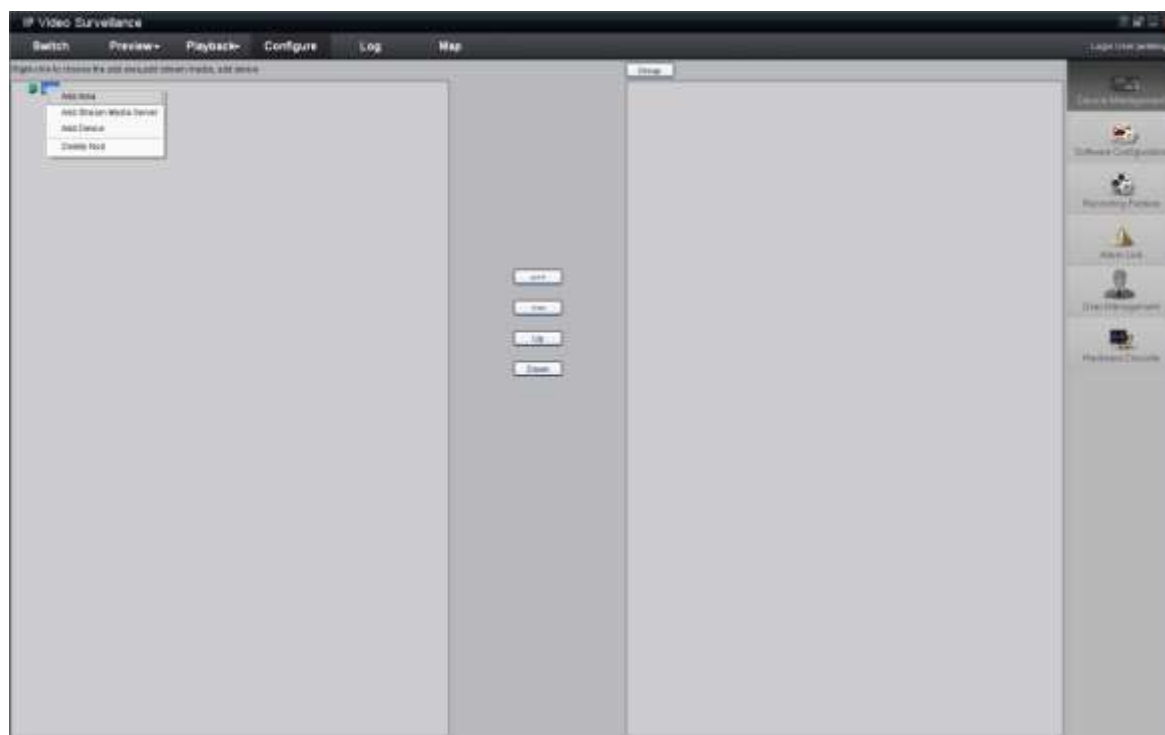


Рисунок 2.12 – Вид экрана после нажатия правой кнопки

При выборе «Add Device», на экране появится окно «Add Device» (Добавление устройства) (см. рисунок 2.12). Выполнить ввод «Device Name» (Имя устройства). Укажите «Normal» из опции «Register». При вводе IP-камеры в «Device IP», например, 192.0.0.64; «User Name»: admin, «Password»: 12345, и порт по умолчанию 8000 в «Port», установить значение «Channel» в 1, выбрать «OK» (Рисунок 2.13).

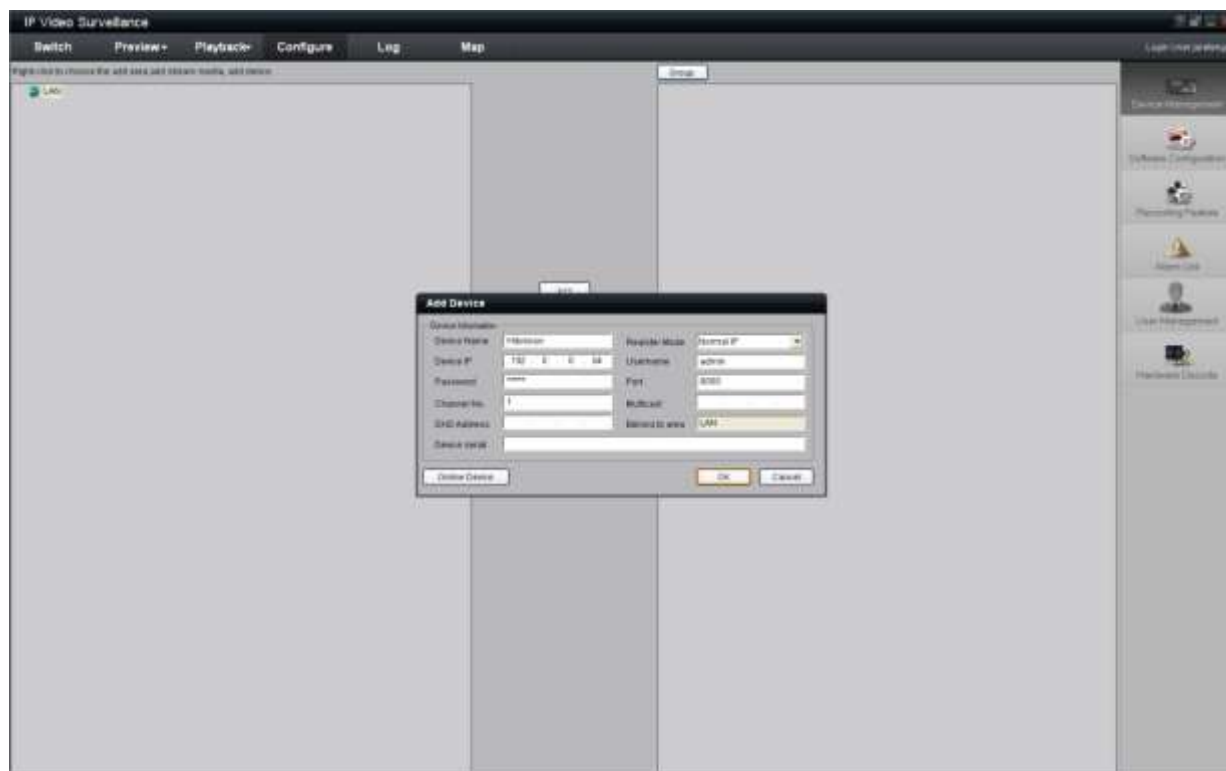


Рисунок 2.13 – Добавление устройства

После успешной выполненной операции, в левой части программы отобразится добавленная и настроенная камера (Рисунок 2.14).

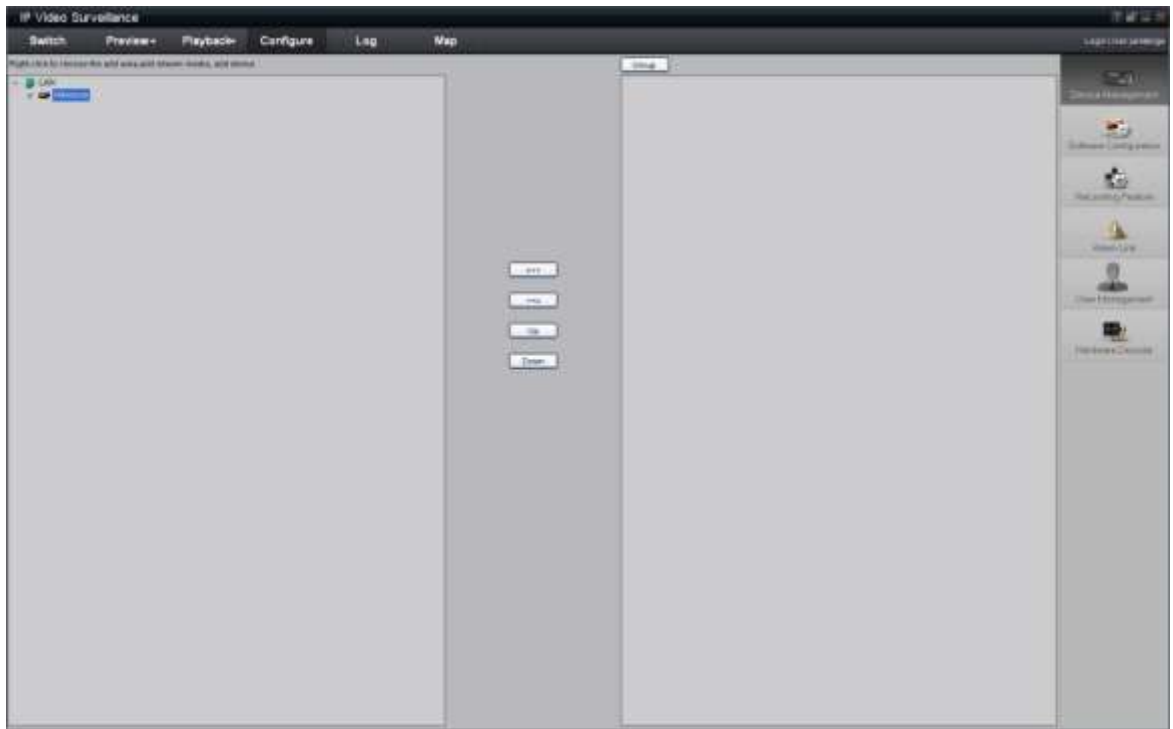


Рисунок 2.14 – Добавление камеры успешно завершено

Выполнить операцию «Preview» для входа в меню предпросмотра «Preview». При двойном нажатии на название камеры получаем окно предварительного просмотра (Рисунок 2.15).

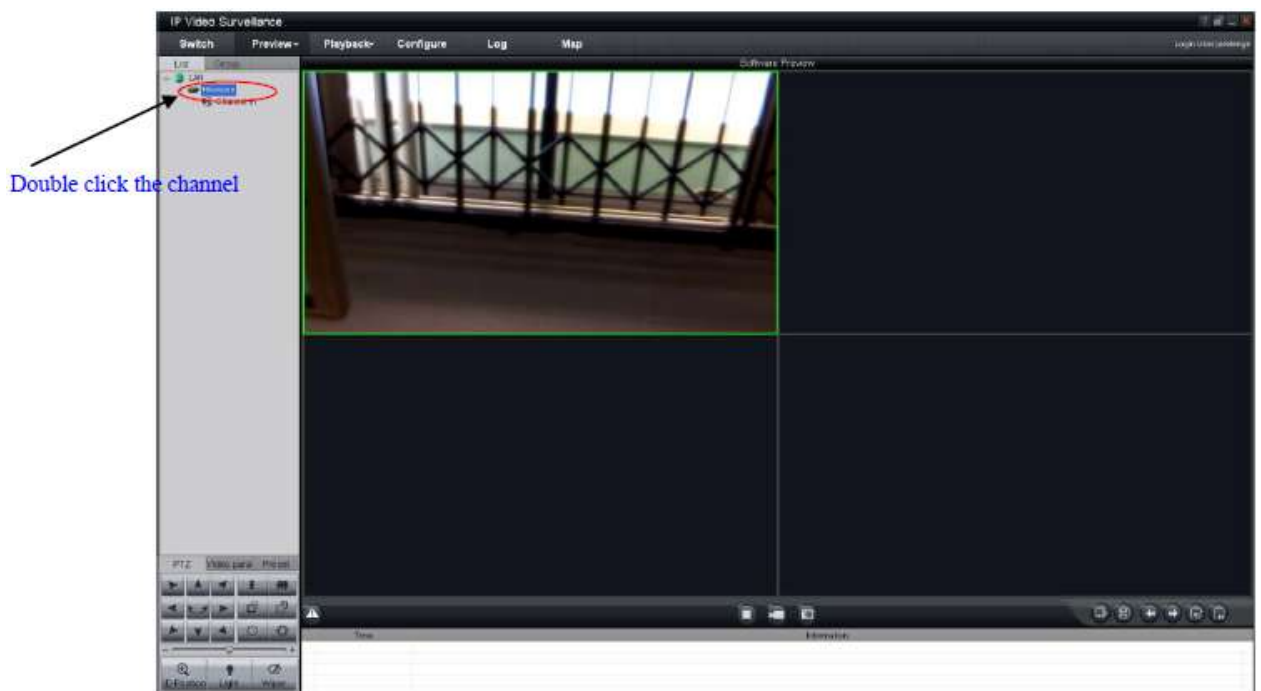


Рисунок 2.15 – Предпросмотр настроенной картинки

Ознакомьтесь с документом «Client Software-4000(v2.0)_ENG.pdf» для дополнительной информации. Данный файл можно найти по адресу «Start» → «All Programs» → «Client Software 4000 (v. 2.0)», который будет создан после установки ПО на компьютер. [14]

Выводы по разделу два:

В данном разделе подобраны наиболее подходящие под наши задачи камеры видеонаблюдения, коммутатор и линия связи между видеокамерами и коммутатором. Рассмотрены структурная и функциональная схемы системы видеонаблюдения. Описана настройка системы видеонаблюдения.

3 ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКИЙ РАЗДЕЛ

Необходимо провести анализ всех затрат при проектировании, разработке и установке системы видеонаблюдения. Полученные данные позволят говорить об эффективности внедрения разработанной системы. Затраты на этапе проектирования и разработки приведены в таблице 3.1.

Таблица 3.1 – Затраты при проектировании и разработке

Наименование работы	Ответственное лицо	Оплата труда, руб/день	Длительность работ, дней	Трудовые затраты, руб.
Получение и анализ технического задания	Инженер	1500	1	1500
Выбор и анализ литературы	Инженер	1500	1	1000
Разработка системы видеонаблюдения	Инженер	1500	3	4500
Закупка и поставка аппаратуры	Инженер	1500	2	3000
Оформление технической документации	Инженер	1500	1	1500
Транспортные расходы	Водитель	1000	2	2000
Итого			11	13500

Затраты на выбранное оборудование в ходе разработке системы видеонаблюдения приведены в таблице 3.2.

Таблица 3.2 – Затраты на оборудование

№	Наименование и техническая характеристика оборудования и материалов	Кол-во, шт.	Цена, руб/шт	Сумма, руб.
1	Персональный компьютер оператора	1	40000	40000
2	Коммутатор HPE V1910-24G-PoE+ JG539A	1	26299	26299
3	Купольная IP-камера Amatek AC-IDV203VA(2,8-12)	10	6570	65700
4	Разъем FinePower RJ45 кат.6 8P8C	22	6,60	145
5	Кабель (SkyNet CSL-FTP-4-CU-OUT) для внешней прокладки	200	21	4200

Продолжение таблицы 3.2

№	Наименование и техническая характеристика оборудования и материалов	Кол-во, шт.	Цена, руб/шт	Сумма, руб.
6	Кабель (SkyNet CSL-FTP-4-CU для внутренней прокладки)	200	21	4200
7	Труба гофрированная ПНД d 16 с зондом	200	12	2400
8	Кабель-канал 16x16	150	12	1800
			Итого	144744

Затраты на монтаж, пуско-наладку и настройку системы видеонаблюдения представлены в таблице 3.3.

Таблица 3.3 – Затраты на монтаж и пусконаладочные работы системы

Вид выполняемой работы	Исполнитель	Кол-во часов	Оплата труда, руб/час	Стоимость, руб
Монтаж и подключение системы видеонаблюдения	Монтажник	24	150	3600
Пусконаладочные работы	Инженер по наладке и испытаниям	4	250	1000
			Итого	4600

Расчет себестоимости системы видеонаблюдения для малого офиса приведен в таблице 3.4.

Таблица 3.4 – Расчет себестоимости системы видеонаблюдения

№	Статья затрат	Сумма затрат
1	Проектирование системы видеонаблюдения	13500
2	Оборудование	144744
3	Заработная плата за установку системы	4600
4	Накладные расходы.	5000
Итого		167844

Общая себестоимость системы видеонаблюдения составит 167844 рублей.

Произведем расчет стоимости функционирования системы видеонаблюдения за 1 год.

Обслуживающим персоналом созданной системы являются инженер, который следит за неполадками в системе. В среднем это будет занимать

2 часа в неделю. Среднегодовая заработная плата инженера за обслуживание системы составляет:

- стоимость часа работы инженера – 250 рублей;
- количество часов на обслуживание в неделю – 1;
- количество недель году – 52.

Исходя из вышеизложенного, следует сделать вывод, что обслуживание системы видеонаблюдения инженером составит: $(250 \text{ рублей} \times 1 \text{ час}) \times 52 \text{ недели} = 13000 \text{ руб/год}$.

Затраты на электроэнергию составят: стоимость 1 кВт электроэнергии составляет – 3,89 рублей.

Потребление электроэнергии системой видеонаблюдения составляет:

- коммутатор – 220 Вт/ч (так как у нас задействовано 10 камер из 24 возможных, то потребление составит 92 Вт/ч);
- персональный компьютер оператора – 50 Вт/ч.

Система видеонаблюдения будет работать непрерывно, за исключением ситуаций в которых будет производиться отключение электроэнергии в ходе проведения сторонних работ (ремонт ЛЭП, ремонт самой системы и т.д.). Примем равным, что таких дней будет 5 за 1 год.

Рассчитаем затраты на электроэнергию системы видеонаблюдения:

$$((92 \text{ Вт/ч} + 50 \text{ Вт/ч}) \times 24 \text{ часа}) \times 360 \text{ дней} = 465120 \text{ Вт/год} = 465,12 \text{ кВт/год}.$$
$$465,12 \text{ кВт/год} \times 3,89 \text{ руб} = 1809,32 \text{ руб/год}.$$

Общие затраты на функционирование системы видеонаблюдения составят:

- обслуживание – 13000 руб/год;
- потребление электроэнергии – 1809.32 руб/год.

$$13000 + 1809.32 = 14809,32 \text{ руб/год. [15]}$$

Выводы по разделу три:

В данном разделе рассчитана себестоимость внедрения системы видеонаблюдения, включающая в себя затраты на проектирование и закупку необходимого оборудования. А так же подсчитаны затраты на монтаж, пуско-наладку, и настройку данной системы видеонаблюдения. Рассчитана стоимость функционирования и годового содержания.

4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Система видеонаблюдения для защиты объекта состоит из нескольких электронных приборов, её стабильная и надежная эксплуатация будет зависеть от многих факторов, как внешних, так и внутренних.

Таким образом, исследовав причины отказа системы защиты, мы сможем увеличить надежность и стабильность работы системы по многим параметрам. Рассмотрим возможные причины выхода из строя рассматриваемой нами системы.

Первой причиной изначально может явиться появление механических повреждений при транспортировке системы. Данная причина не является обязательной и часто встречаемой.

Вторую причину определим как неверную схему установки системы на объекте. Данное обстоятельство довольно распространено и зависит от квалификации установщика.

Третья, возможная причина выхода из строя системы – это неправильная эксплуатация данной системы. Человек по многим причинам может являться угрозой для рассматриваемой системы.

Четвертой причиной можно назвать довольно распространенную для всех электронных приборов – это неустойчивая подача напряжения в сети. От данной угрозы ни одна электронная система не застрахована.

И пятая причина выхода из строя рассматриваемой системы, которая не зависит от поведения потребителя, является брак завода-изготовителя. От того какую систему мы изначально приобретем для защиты того или иного периметра, зависит результат.

Рассматривая причины выхода из строя прибора необходимо строго соблюсти последовательность этих причин, чтобы выяснить общую картину отказов.

Первой причиной для нашей системы мы определили механические повреждения, которые в свою очередь не зависят от потребителя, а строго от фирмы поставщика.

Вторая причина – неверная схема установки системы на объекте может включать в себя как невнимательную сборку установщиком, так и преждевременное тестирование системы. Последнее может быть из-за попытки сократить срок установки системы фирмой-подрядчиком, а именно:

- из-за отсутствия первоначального осмотра объекта охраны;
- начат этап монтажа, в то время как не завершен этап уточнения параметров системы при проектировании.

Третьей причиной отказа мы определили неправильную эксплуатацию прибора. А так же определили главную некорректность. И ей является несоблюдение оператором инструкции по эксплуатации системы. Но этого объяснения не достаточно, хотя оно является всеобъемлющим, т.к. инструкции по эксплуатации прилагаются к любой системе и ее соблюдение является строгой необходимостью. Поэтому неправильная эксплуатация системы может возникнуть из-за невнимательной работы оператора из-за отсутствия навыка работы.

Еще одной причиной выхода из строя системы ввиду неправильной эксплуатации, были определены условия, в которых работает оператор, прежде всего, могут отсутствовать элементарные условия труда, вызванные низкой освещенностью автоматизированного рабочего места (далее – АРМ) оператора, недостаточная вентиляция пункта охраны и несоблюдение эргономических требований к АРМ. Так же сам оператор может не иметь надлежащий квалификации и навыков по обращению с элементами системы.

Следующей причиной является проникновение постороннего на пункт охраны. Данную проблему можно рассмотреть еще с нескольких сторон: человек случайно попал на пункт охраны (это не исключено, если объект охраны не является секретным, или если же на пропускном пункте не было проявлено достаточной бдительности).

Но может быть другой случай: человек, проникший на пульт охраны, является злоумышленником (т.е. его появление на данном охраняемом объекте не случайно).

В результате такого проникновения могут возникнуть сразу же две неизбежные угрозы:

- злоумышленник вывел из строя систему защиты отключения видеосистемы наблюдения или систему контроля допуска путем ее отключения;
- злоумышленником был осуществлен акт вандализма по отношению к видеокамерам.

Рассмотренные угрозы могут существовать как отдельно друг от друга, так и вместе.

Четвертую причину мы определили, как неустойчивую подачу напряжения в сети. Причин может быть несколько:

- отсутствует напряжение в сети;
- напряжение выше нормы.

Вторая причина не зависит от потребителя, поэтому рассмотрим первую причину. Отсутствие напряжения в сети может быть вызвано:

- отсутствием источника резервного питания системы;
- разрядом источника резервного питания при его наличии;
- отсутствием энергоснабжения объекта, вызванные проблемами поставки электроэнергии у энергоснабжающей организации.

Резервное питание из-за экономии средств могут не устанавливать. Так же бывает, что резервный аккумулятор садится, а технический оператор этот момент не проконтролировал, поэтому может тоже случиться отказ системы.

Пятой причиной мы определим брак завода-изготовителя, который не зависит от потребителя, а зависит от фирмы-поставщика.

Охрана окружающей среды в настоящее время стала одной из насущных проблем. Технологические процессы производства всех отраслей промышленности неразрывно связаны с потреблением природных ресурсов, и разнообразными выбросами в окружающую среду жидких, твердых, газообразных отходов.

При разработке и эксплуатации системы, опасности загрязнения экосистемы не возникает. Это возможно в силу того, что блок не выделяет вредных веществ при своей работе, не радиоактивен, уровень электромагнитного излучения не опасен для человека и природы.

Поэтому рассмотрим более подробно защиту окружающей среды на этапе изготовления и утилизации устройств и элементов системы.

При изготовлении наибольшую опасность представляет загрязнение атмосферы отходами производства. Такими отходами являются токсичные газы (оксид углерода, фтористый водород) и аэрозоли (свинец и его соединения), которые выделяются при проведении монтажных работ. Эти вещества, попадая внутрь человека, приводят к нарушению его здоровья. Так, оксид углерода, попадая через органы дыхания в организм, действуют на нервную и сердечно-сосудистую системы, вызывая удушье. Под воздействием свинца нарушается синтез гемоглобина, работа мочеполовых органов, нервной системы. Для предотвращения острых и профессиональных заболеваний содержание свинца в воздушной среде не должно превышать предельно допустимой концентрации – 0,01 мг/м³.

В этом случае в рабочей зоне воздух находится в состоянии насыщения вредными элементами, а удаляемый из помещений вентиляционный воздух может стать причиной загрязнения атмосферного воздуха.

Для предотвращения этого используются различные методы защиты атмосферы. Основными из них являются: локализация токсичных веществ у источников загрязнения и очистка загрязненного воздуха. В свою очередь эти методы представляют целый набор мероприятий по очищению окружающей среды. Устройства для локализации примесей представляют собой местные отсосы и укрытия с отсосами. В тех случаях, когда источник вредных выбросов заключен внутри пространства, огражденного жесткими стенками, отсосы выполняются в виде вытяжных шкафов, кожухов, витринных отсосов. Если по условиям технологии или обслуживания источник вредности нельзя заключить в кожух, то

над таким источником или около него устанавливается вытяжной зонт. Очистка загрязненного воздуха может осуществляться пылеуловителями (сухими, электрическими, фильтрами), туманоуловителями, аппаратами для улавливания паров и газов и аппаратами многоступенчатой очистки, методы очистки которых основаны на различных физико-химических процессах.

Для предохранения атмосферы от выбросов в неё химических веществ следует применять сухие пылеулавливатели, электрические фильтры Петрянова, для тонкой очистки от газовых выбросов и примесей, рекомендуется использовать стеклоткань ТССНФ.

Также на этапе изготовления существует опасность загрязнения гидросферы отходами производства. При травлении печатных плат в производстве используют различные химические составы (хлорное железо и т.д.), часть которых попадает в сточные воды, следовательно, необходимо разработать очистные мероприятия. В соответствии с видами процессов, происходящих при очистке, все существующие методы принято делить на механические, физико-химические и биологические. При механической очистке сточных вод от взвешенных веществ используют процеживание, отстаивание, фильтрование и т.п. В настоящее время существенно увеличилась роль физико-химических методов (флотация, экстракция, нейтрализация, ионообменная и электрохимическая очистки) в связи с использованием оборотных систем водоснабжения. Биологическая очистка сточных вод применяется для выделения из них тонкодисперсных и растворенных органических веществ, основана на способности микроорганизмов использовать для питания содержащиеся в сточных водах органические вещества (кислоты, спирты, углеводы и т.п.). В нашем случае можно применить электрохимическую очистку и сорбцию для защиты водных ресурсов от загрязнения отходами производства. [15]

На всех этапах изготовления изделия существует опасность загрязнения литосферы, т.к. данное производство не безотходное. При нарезке, пайке, травлении печатных плат, изготовлении и покраске корпуса остаются отходы,

содержащие свинец, олово и их соединения, органические горючие (обтирочные материалы, ветошь, обрезки пластмасс, оргстекла, остатки лакокрасочных материалов), которые необходимо складировать в определенном месте и в дальнейшем отправлять на переработку на полигон. Переработку промышленных отходов производят на специальных полигонах, создаваемых в соответствии с требованиями СНиП 2.01.28-85 «Полигоны по обезвреживанию и захоронению токсичных промышленных отходов. Основные положения по проектированию» [16] и предназначенных для централизованного сбора, обезвреживания и захоронения токсичных отходов.

Опасность литосфере грозит и на этапе утилизации. Но, с учетом того, что практически полностью все элементы и устройства разработанной системы могут быть использованы вторично: корпус возможно использовать для размещения в нем другого устройства, печатная плата может быть разобрана на отдельные элементы и часть из них использована вновь для построения другого устройства. Те элементы, которые не могут быть использованы, например, из-за поломки или истекания срока годности, необходимо складировать в контейнер для утилизации, а затем отправить на переработку на специальный полигон.

Наиболее эффективным методом решения проблемы защиты литосферы от промышленных отходов, является применение безотходных и малоотходных технологий и производств.

Очевидно, что при выполнении требований по защите окружающей среды от загрязнения, никакого вреда экосистеме нанесено не будет.

В качестве методов улучшения условий труда пользователя разработанной системы предлагаются меры, которые можно условно разделить на три группы:

- организационные;
- технические;
- организационно-технические.

В работе с системой обязательно должны присутствовать перерывы, в течение которых пользователь может переключиться на небольшие физические

упражнения, также немаловажно позволять разработчикам выполнять задания, чередуя сложные и менее сложные, кроме того, необходимо соблюдение ряда условий: постепенное вхождение в трудовой процесс после отдыха, индивидуальный ритм работы, соблюдение привычной последовательности деятельности.

Во время перерывов рекомендуется психологическая разгрузка в оборудованных для этой цели помещениях, оборудованных удобными креслами, и звучащей специально подобранной спокойной музыкой, на стенах могут быть изображены пейзажи, оказывающие успокоительное воздействие.

Исследования физиологов и гигиенистов убедительно доказали, что и полутьма, и слишком высокая освещенность экрана приводят к быстрому зрительному утомлению, поэтому размещать компьютер рекомендуется так, чтобы свет (естественный или искусственный) падал сбоку, лучше слева, это избавит от мешающих теней и поможет снизить освещенность экрана.

В качестве источников освещения рекомендуется применять люминесцентные лампы белого цвета со светильниками серии ЛПО36 с зеркализированными решетками.

Одним из способов снижения вредного влияния видеотерминала можно назвать применение в качестве последних жидкокристаллических панелей. Их достоинством является отсутствие электромагнитных излучений и мерцания экрана.

Также следует отметить, что в России наиболее важными являются санитарные правила и нормы (СанПиН) 2.2.2/2.4.1340-03, устанавливающие гигиенические требования к персональным электронно-вычислительным машинам (далее – ПЭВМ) и организации их работы. [17] СанПиН определяют обязательные требования к ПЭВМ (допустимые уровни звукового давления и уровней звука, создаваемого ПЭВМ, допустимые уровни электромагнитных полей, допустимые визуальные параметры устройств отображения, допустимая концентрация вредных веществ, выделяемых ПЭВМ в воздух помещений, максимальная мощность

экспозиционной дозы мягкого рентгеновского излучения) и рабочему месту с ПЭВМ (естественное и искусственное освещение, площадь на одно рабочее место, защитное заземление (зануление), микроклимат, содержанию аэроионов и вредных химических веществ в воздухе, уровни шума и вибрации на рабочих местах, продолжительность непрерывной работы и перерывов, периодичность проветривания и влажной уборки помещений, организация медицинского обслуживания пользователей ПЭВМ). [18]

Таким образом, согласно вышеописанному, можно привести следующие меры по улучшению условий труда, которые указаны в таблице 4.1.

Таблица 4.1 – Факторы, относящиеся к напряженному труду, и соответствующие мероприятия по улучшению условий труда. [19]

Факторы, относящиеся к напряженному труду	Фактическое значение	Класс условий труда	Мероприятия по улучшению условий труда
Микроклимат	Находится в помещении с компьютерами и печатными устройствами	2	Установка кондиционеров, со встроенным увлажнителем воздуха. Покупка бесшумных звукоизолированных корпусов для ПК, и печатного оборудования. Установка ламп дневного света.
Содержание работы	Эвристическая (творческая) деятельность	3.2	Введение регламентированных перерывов длительностью 10 минут через каждый час работы (группа В III)
Восприятие сигналов	Восприятие сигналов с последующим сопоставлением фактических значений параметров с их номинальными значениями. Заключительная оценка фактических значений параметров.	3.2	Выполнение упражнений для глаз (зрительная гимнастика)

Продолжение таблицы 4.1

Факторы, относящиеся к напряженному труду	Фактическое значение	Класс условий труда	Мероприятия по улучшению условий труда
Длительность сосредоточенного наблюдения (% от времени смены)	Более 75%	3.2	Введение регламентированных перерывов длительностью 10 минут через каждый час работы (группа В III).

Выводы по разделу четыре:

В данном разделе рассмотрены вопросы, связанные с тем, что работники вычислительного центра: операторы АРМ, операторы по подготовке данных, программисты подвергаются воздействию физически опасных и вредных производственных факторов таких, как повышенный уровень шумов, отсутствие или недостаток естественного света, недостаточная освещенность рабочей зоны и др. Определены пути решения этих проблем, чтобы обеспечить безопасные условия труда для работников вычислительного центра. Особое внимание уделяется пожарной безопасности, так как пожары в вычислительном центре сопряжены с опасностью для человеческой жизни и большими материальными потерями.

ЗАКЛЮЧЕНИЕ

Используя передовые технологии, современное качественное оборудование и материалы для монтажа, можно получить надёжную и простую в эксплуатации систему видеонаблюдения.

Благодаря определению условий эксплуатации (был построен ряд зависимостей, влияющих на выбор видеокамер для конкретных систем видеонаблюдения, а именно зависимости угла обзора видеокамеры и фокусного расстояния видеокамеры от дальности), также было произведено обоснование выбора оборудования для системы IP-видеонаблюдения, было определено требуемое количество видеокамер, их расстановка, были рассчитаны необходимые и дополнительные параметры для выбора видеокамер, было выбрано оборудование для будущей системы IP-видеонаблюдения, разработана структурная схема данной системы и электрическая принципиальная схемы соединений (учитывая структуру IP системы видеонаблюдения и план территории, была построена структурная схема разрабатываемой системы видеонаблюдения).

Таким образом, были решены задачи, связанные с определением современного состояния и тенденций системы IP-видеонаблюдения, были определены преимущества, эффективность, возможности, перспективы развития и удобство использования таких систем, также был определен состав системы IP-видеонаблюдения, классификация видеокамер и ПЗС-матриц.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

- 1 Гвоздек, М. Справочник по технике для видеонаблюдения. Планирование, проектирование, монтаж / М. Гвоздек. – М.: Техносфера, 2016. – 552 с.
- 2 Кашкаров, А. П. Системы видеонаблюдения. Практикум / А.П. Кашкаров. – М.: Феникс, 2016. – 128 с.
- 3 Хомоненко А.Д. Основы современных компьютерных технологий//Учебное пособие для вузов. – С-Пбт: Корона принт, 2015. Витая пара
- 4 Беспроводные сети Wi-Fi. - М.: Интернет-университет информационных технологий, Бинум. Лаборатория знаний, 2013. - 216 с.
- 5 Системы телевизионного наблюдения. / Никулин О.Ю., Петрушин А.Н. - Ай-Эс-Эс Пресс, 2002. – 322 с. 24. Скрытая камера: Журнал. М.: Тинко, 2016. – №12 – 54 с. 25.
- 6 Брайан Хилл Глава 9. Основные сведения о коммутаторах // Полный справочник по Cisco = Cisco: The Complete Reference. — М.: «Вильямс». — С. 1088. — ISBN 0-07-219280-1
- 7 Кругль Г.Д. Профессиональное видеонаблюдение. Практика и технологии аналогового и цифрового CCTV. – М.: «Медиа Фокус», 2015. – 672 с.: ил.
- 8 Выбор и установка системы видеонаблюдения. Статья. – [дата обращения – 02.02.2018.].
- 9 Пескин, А. Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации / А.Е. Пескин. – М.: Горячая линия – Телеком, 2014. – 256 с.
- 10 Рассел, Джесси Видеонаблюдение / Джесси Рассел. – М.: Книга по Требованию, 2016. – 106 с.
- 11 Магауенов Р.Г. Системы охранной сигнализации. Основные теории и принципы построения. – М.: Горячая линия – Телеком, 2016. – 508 с.

12 РД 78.36.003-2016 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств».

13 Скрытая камера: Журнал.М.: Тинко, 2017. – №8 – 62 с. 28. Уокер Ф. Электронные системы охраны: перев. с англ. – М.: За и против, 2016. – 164 с. 29. Р 78.36.008-99 «Рекомендации. Проектирование и монтаж систем охранного телевидения и домофонов».

14 Кругль Г. Профессиональное видеонаблюдение. Практика и технологии аналогового и цифрового CCTV. – М.: Секьюрити Фокус, 2010. – 640 с.

15 СНиП 2.01.28-85 «Полигоны по обезвреживанию и захоронению токсичных промышленных отходов. Основные положения по проектированию» 2015, с. 360 с.

16 Дамьяновски В. CCTV. Библия видеонаблюдения. Цифровые и сетевые технологии. – М.: Ай – Эс – Эс Пресс, 207 год, – 280 с.

17 (СанПиН) 2.2.2/2.4.1340-03, устанавливающие гигиенические требования к персональным электронно-вычислительным машинам (далее – ПЭВМ) и организации их работы. 2015, с. 300 с.

18 Воронов В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: Горячая линия – Телеком, 2015. – 272 с.

19 Организация и современные методы защиты информации. Информационно-справочное пособие. - М.: Ассоциация "Безопасность", 2015, с. 440 с.

20 Буйлушкина, Л.Н. Методические рекомендации по подготовке и оформлению выпускной квалификационной работы (проекта) для технических направлений подготовки 09.03.01 Информатика и вычислительная техника, 09.03.04 Программная инженерия, 12.03.01 Приборостроение, 23.03.01 Технология транспортных процессов / Л.Н. Буйлушкина. – Нижневартовск, 2017. – 35с.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ А. КОМПАКТ-ДИСК

Содержание:

1. Пояснительная записка.
2. Презентация.